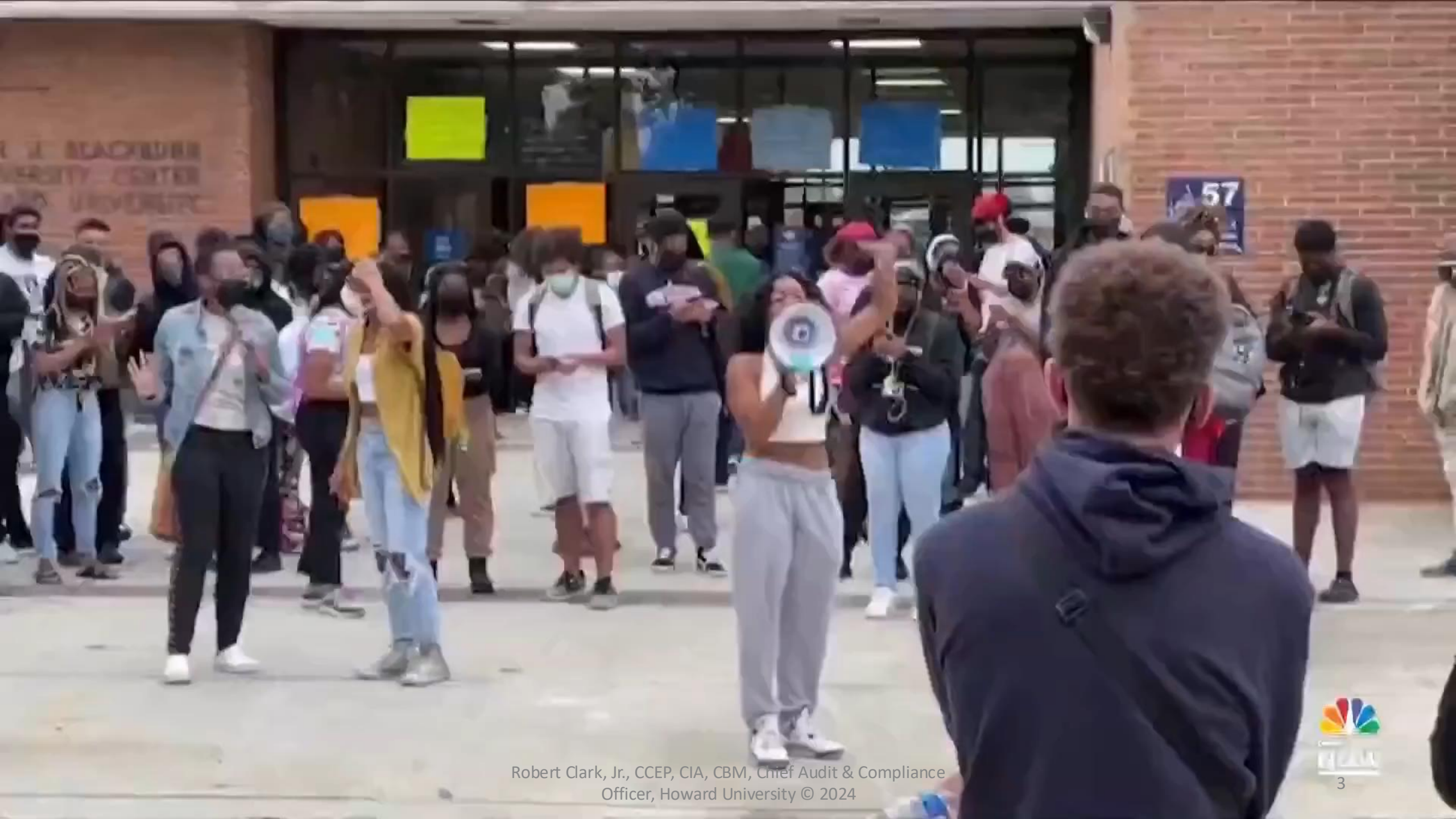
Rob Clark, Jr., CIA, CCEP, CBM, CVP
Chief Audit & Compliance Officer
Howard University
robert.clark@howard.edu
https://www.linkedin.com/in/robclarkjr/
www.RobClarkJr.com
770.815.7922

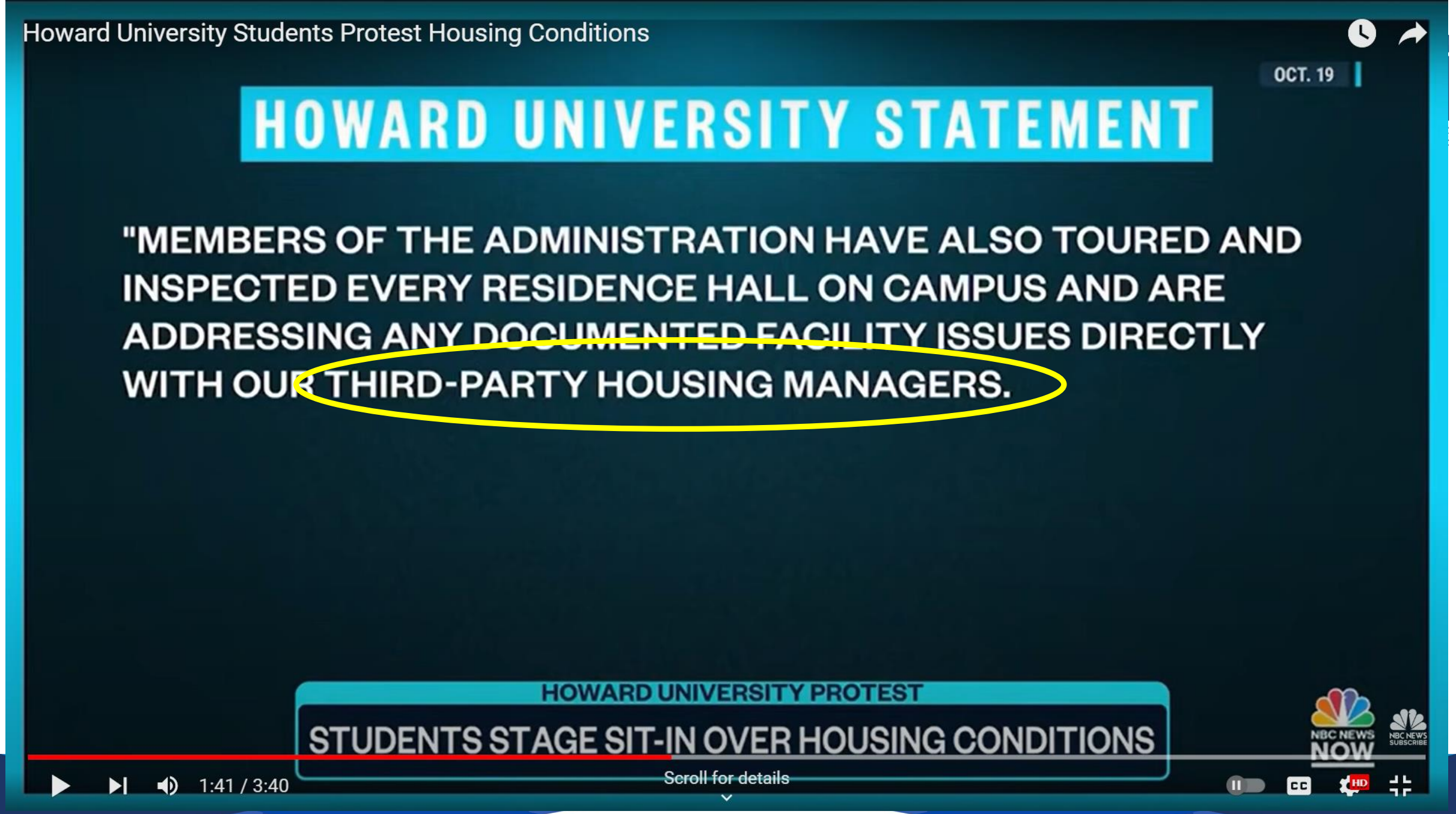
Third-Party Risk Management & Contracting

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

UK Auxiliary Services


57



Objectives of the Session

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

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?

What is your role in managing contracts?

[SLIDO INSERT]:
What is your role in managing contracts?

1) No clue… I leave that up to the Purchasing and Legal folks
2) I have some responsibility to monitor that contracts are followed
3) I am involved in the whole shebang – from negotiating the contract to monitoring for compliance
4) I'm part of a team that manages the contract process
5) I monitor the effectiveness of how the contract is being managed by the responsible unit(s)

COSO Framework: Enterprise Risk Management

"Enterprise Risk Management -- Integrating with Strategy and Performance"

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

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?

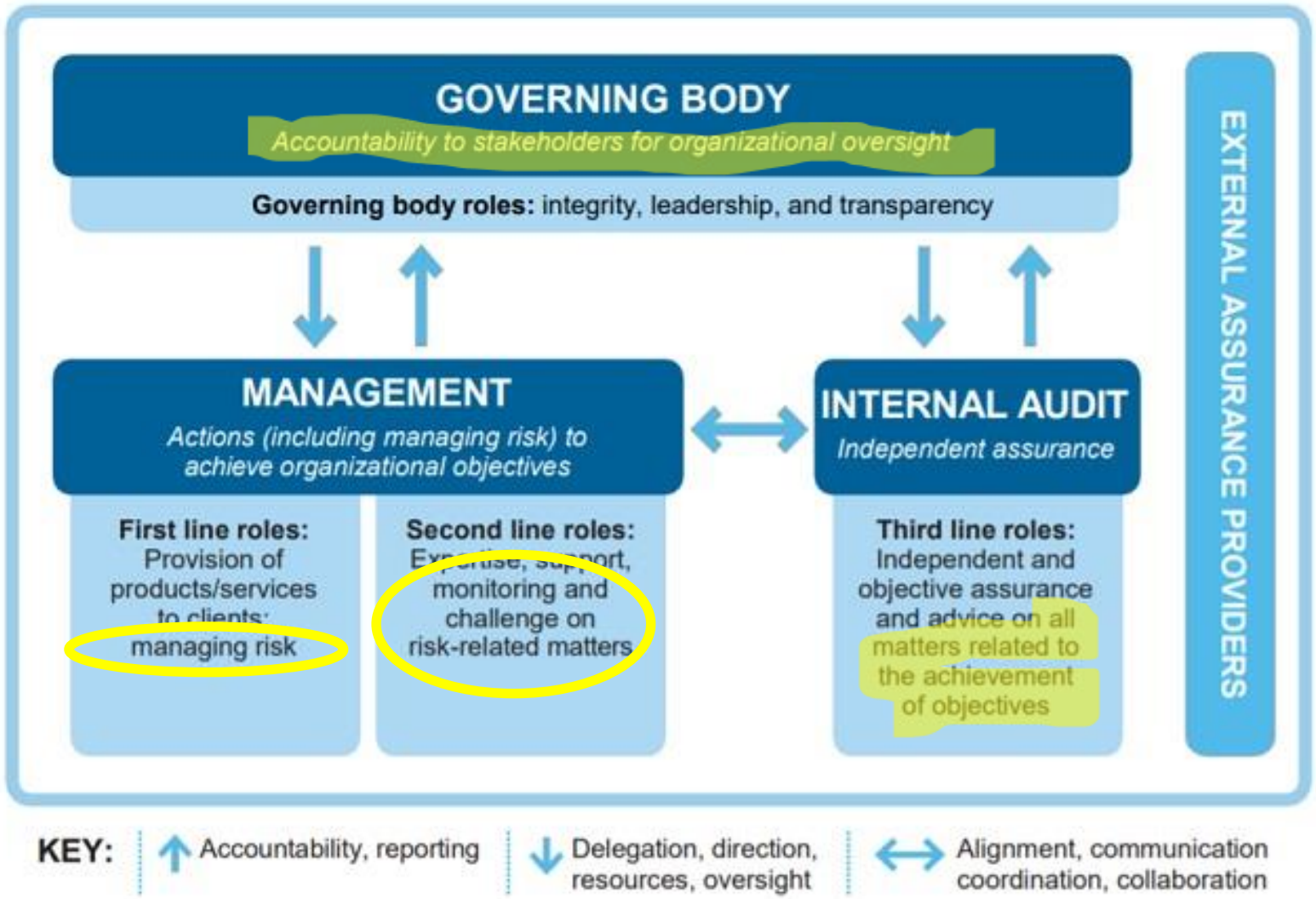
How to manage risk: Share it, avoid it, reduce it, or accept it

Procedures to ensure effective risk mitigation

Education & awareness of effective policies and practices

Management reviews & audit assesses

The IIA's Three Lines Model



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			
				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**

How many third-party vendors do you have at your institution?

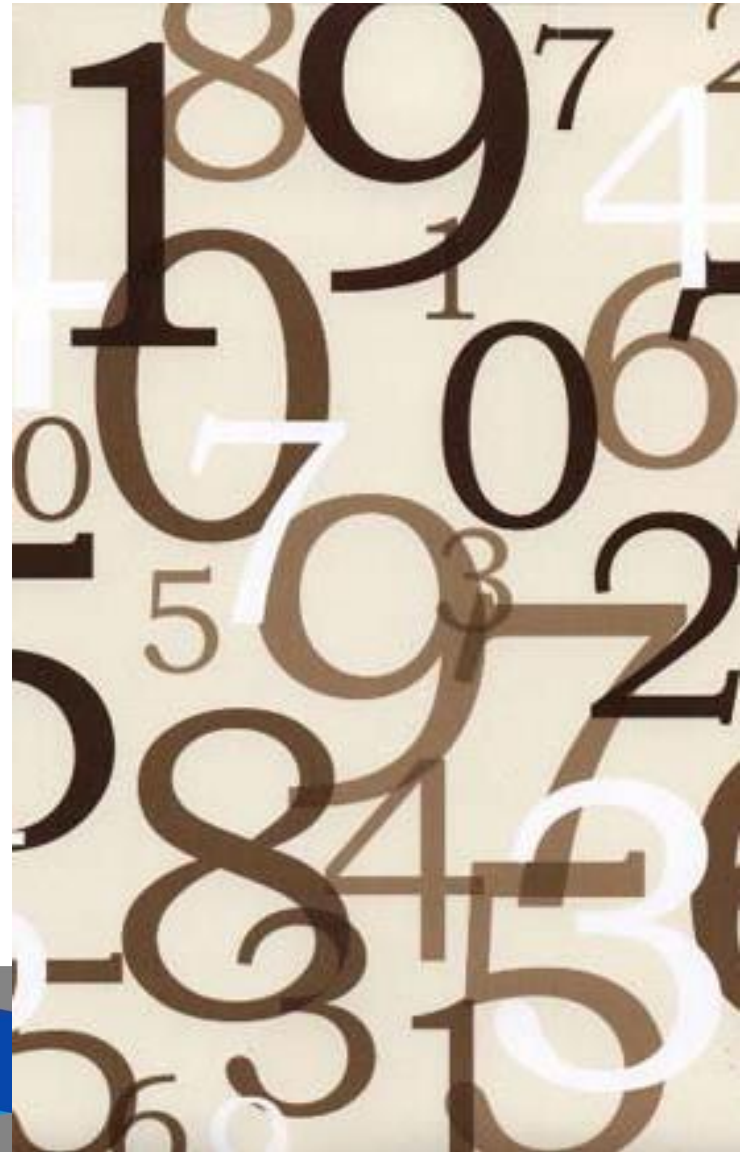
[SLIDO INSERT]

How many third-party vendors do you have at your institution?

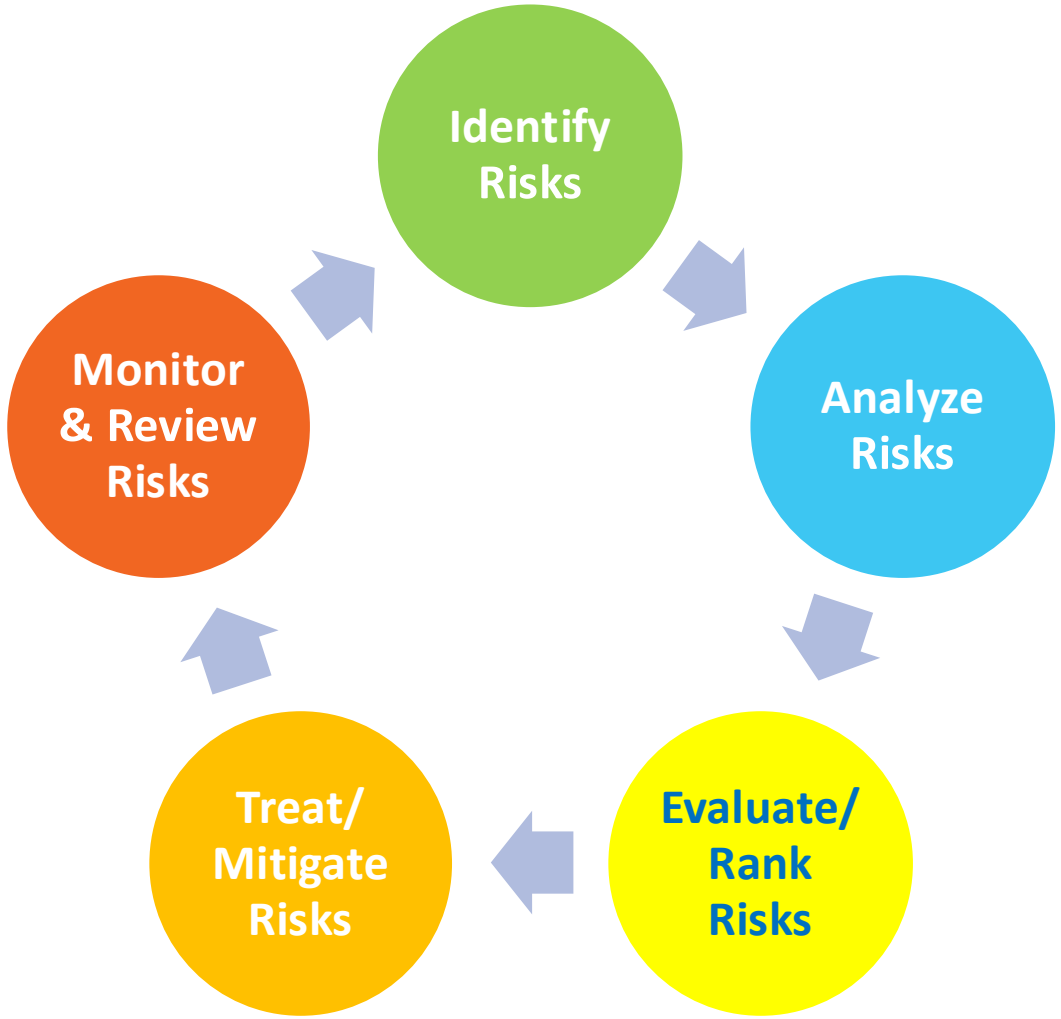
1) **1 – 100**
2) **101 – 500**
3) **501 – 1,000**
4) **1,000 +**

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



5 Phases of Third-Party Monitoring

1) Planning & Risk Assessment

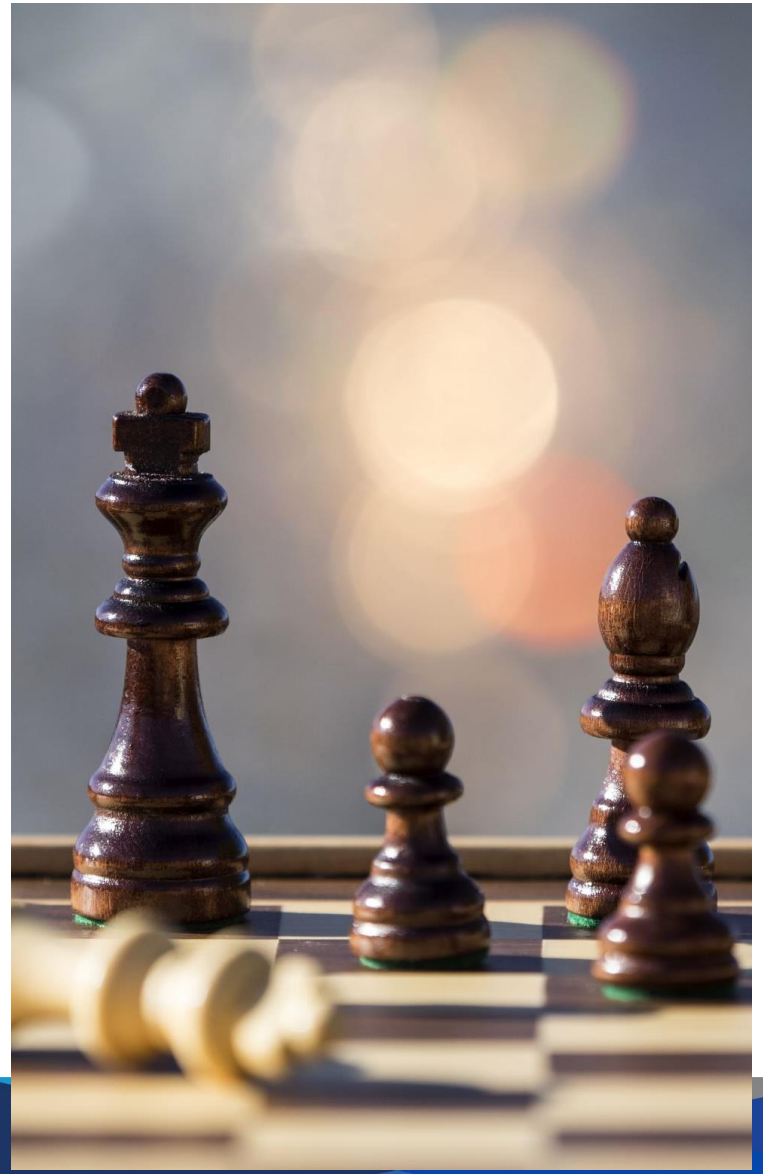
Who is involved?

- Business owner who would manage day-to-day activities of vendor
- IT (CIO, CISO, CTO)
- Legal
- CFO
- Procurement
- 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 an organization. The council typically consists of senior leaders, executives, and representatives from various business units and functions within the organization.

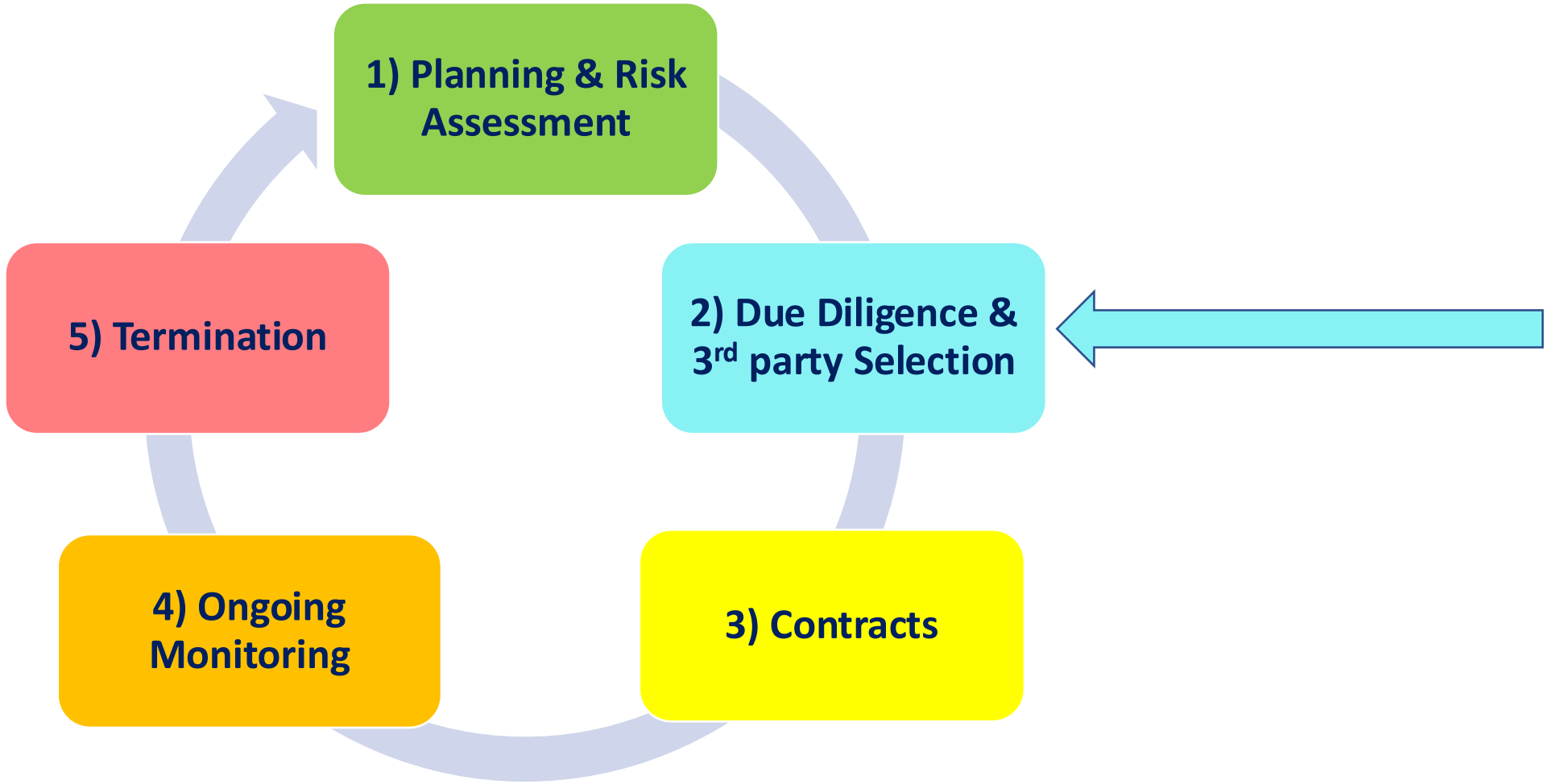
Focus of IT Governance Council

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 oversees the allocation of IT resources, including budget, personnel, and technology infrastructure. It evaluates proposals for IT projects and initiatives, making decisions on priorities, funding, and resource allocation.

Focus of IT Governance Council

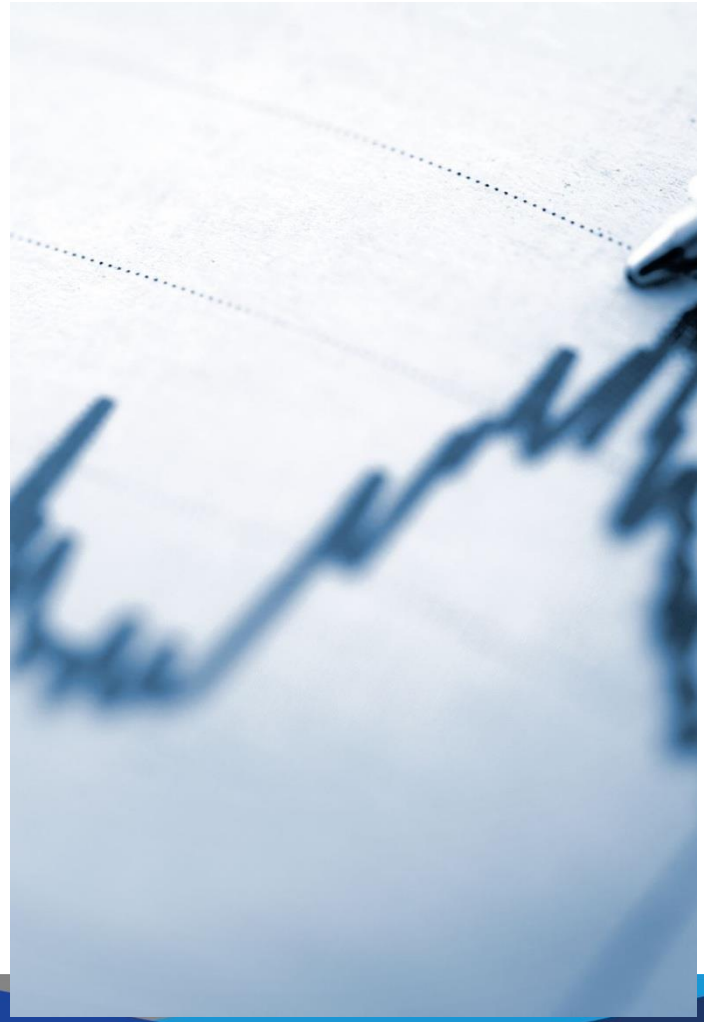
4) **IT policy development**: The council establishes and reviews IT policies, standards, and guidelines to ensure compliance, consistency, and best practices across the organization. It helps develop IT governance frameworks, frameworks for data management, and cybersecurity protocols.
5) **Performance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



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

SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users' 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

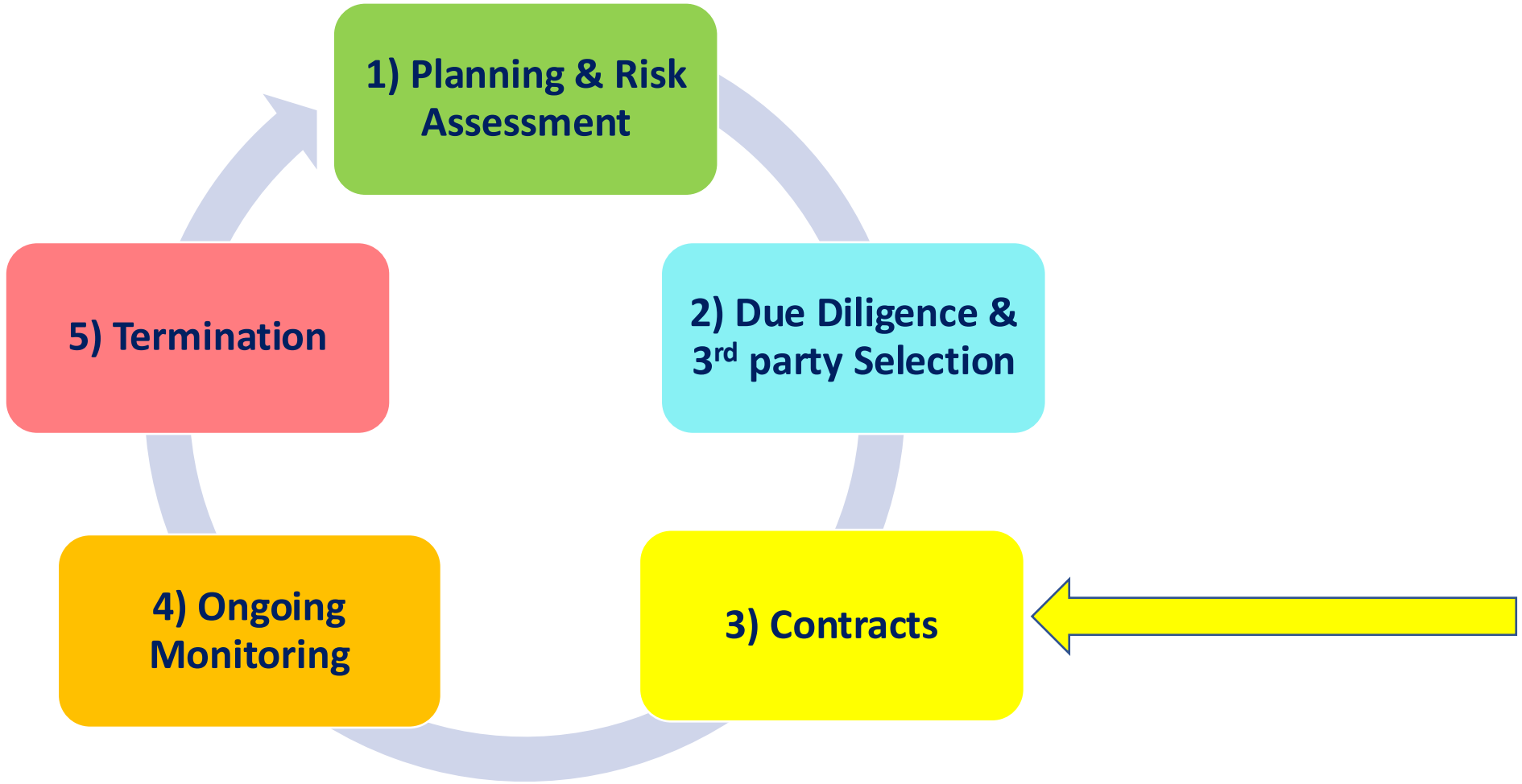
Check CSPs with STAR Registry

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.)

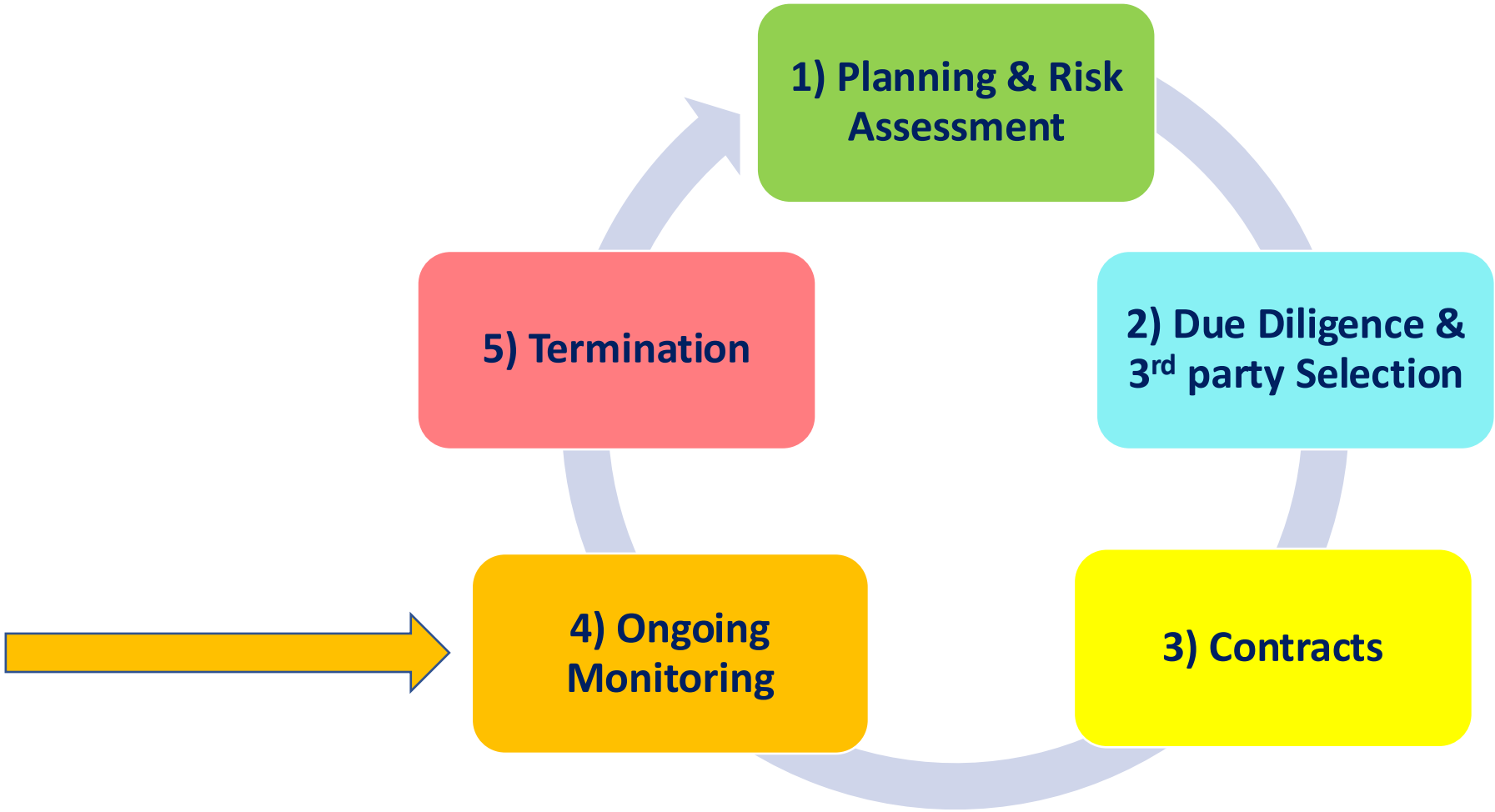
5 Phases of Third-Party Monitoring



3) Contracting

- Business Continuity and Disaster Recovery
- Data ownership and liability
- Information security and privacy requirements (including breach notification)
- Right to audit (questionnaires, interviews, audits)
- Scope of services
- Service level agreements
- Subcontractor relationships
- Termination events

5 Phases of Third-Party Monitoring



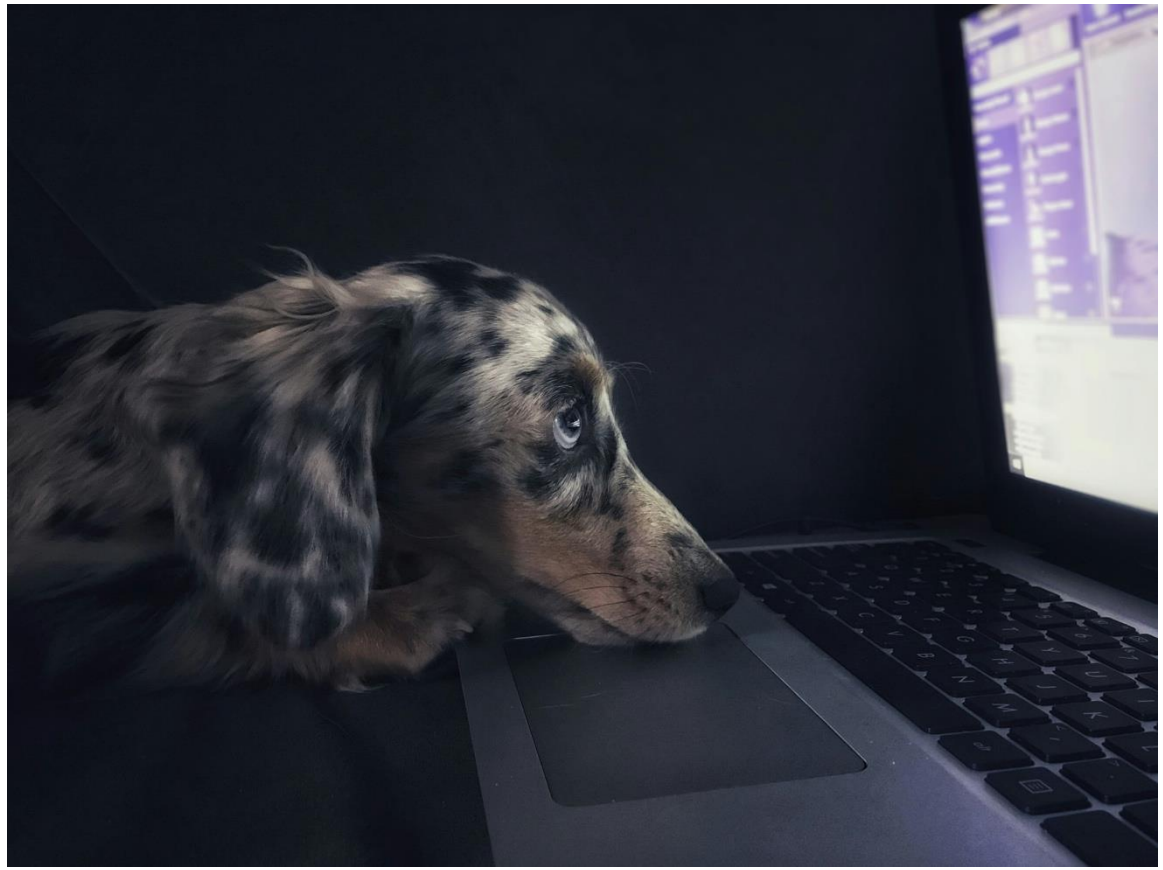
4) Ongoing Monitoring

For critical third-parties, regulators expect:

- Due diligence specific and commensurate to each vendor
- Robust monitoring
- Holding vendor accountable to adhere to terms and conditions
- Escalating issues on non-conformance
- Documentation and reports of activities

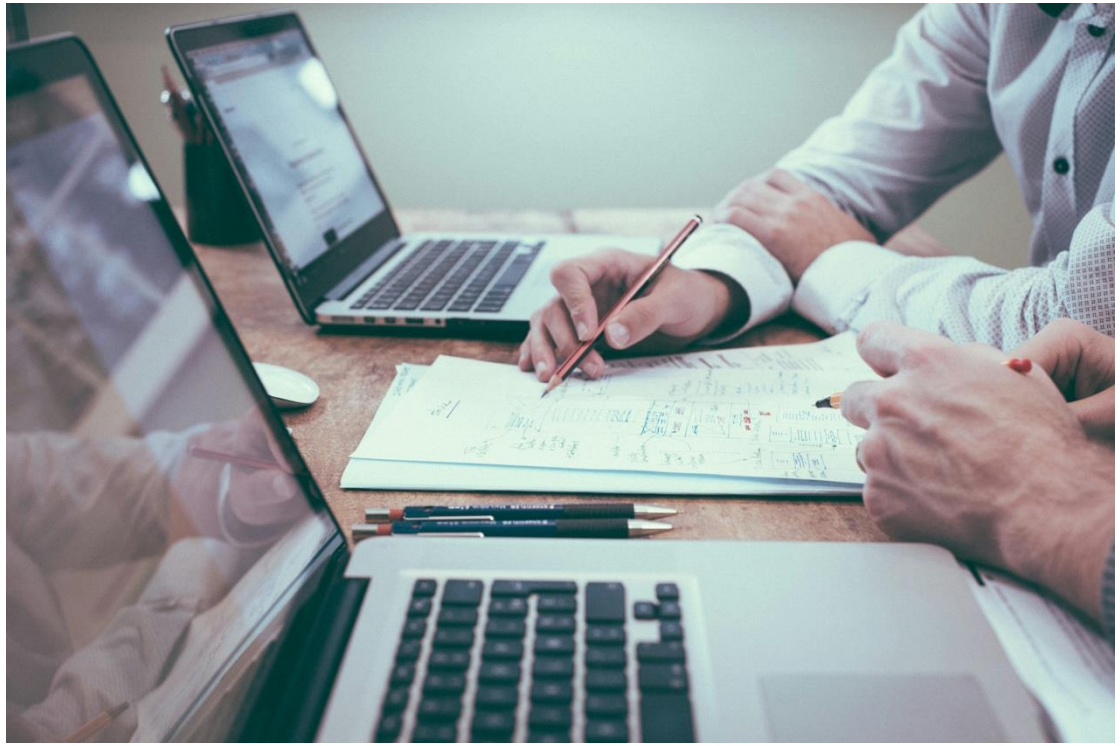
4) Ongoing Monitoring

- Continuous monitoring
- Point-in-time monitoring
- Risk re-assessments
- Structured third-party offboarding

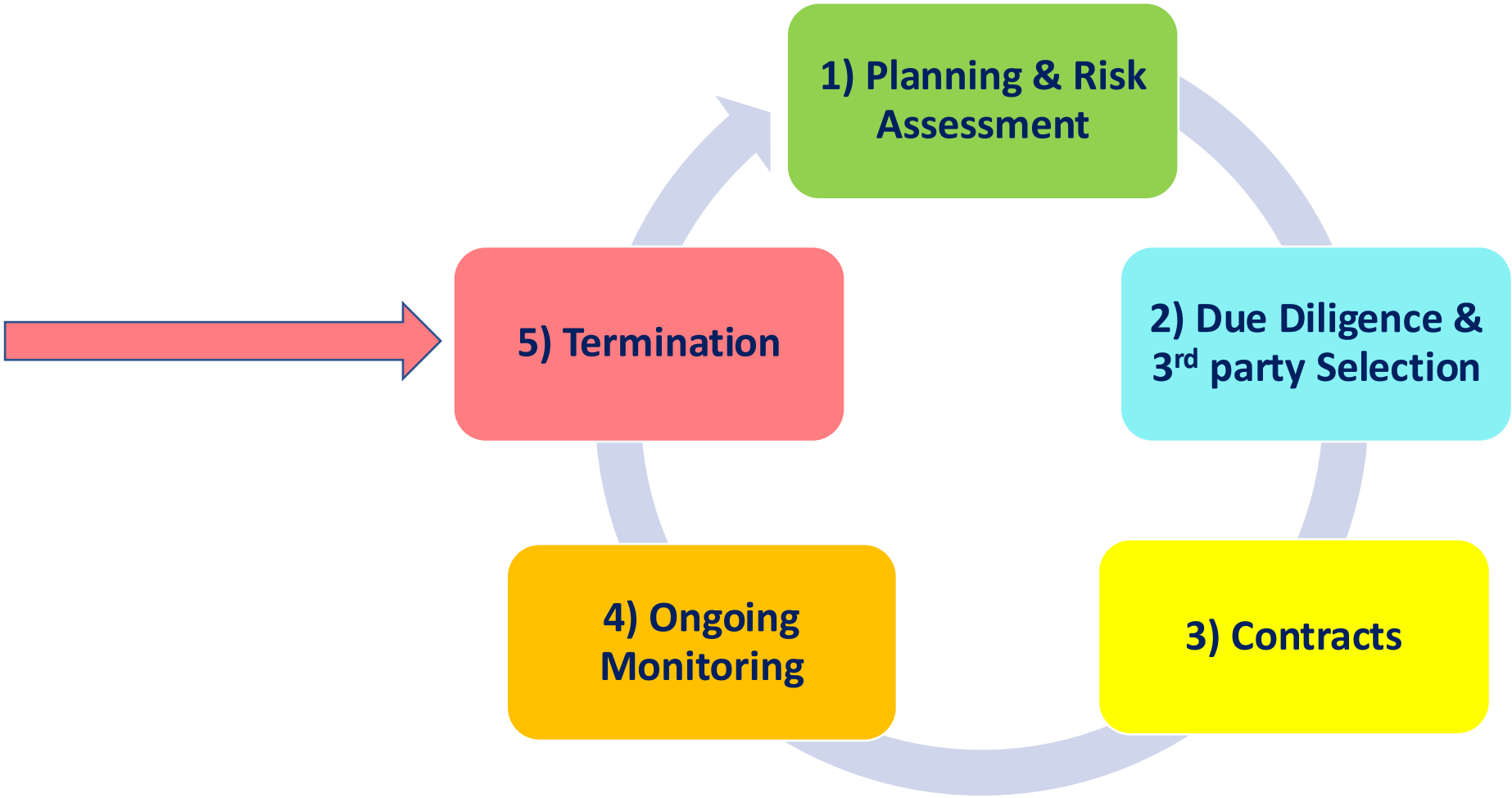


4) Ongoing Monitoring – What to Monitor

- Business strategy and reputation
- Compliance with legal and regulatory
- 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 third-parties



5 Phases of Third-Party Monitoring



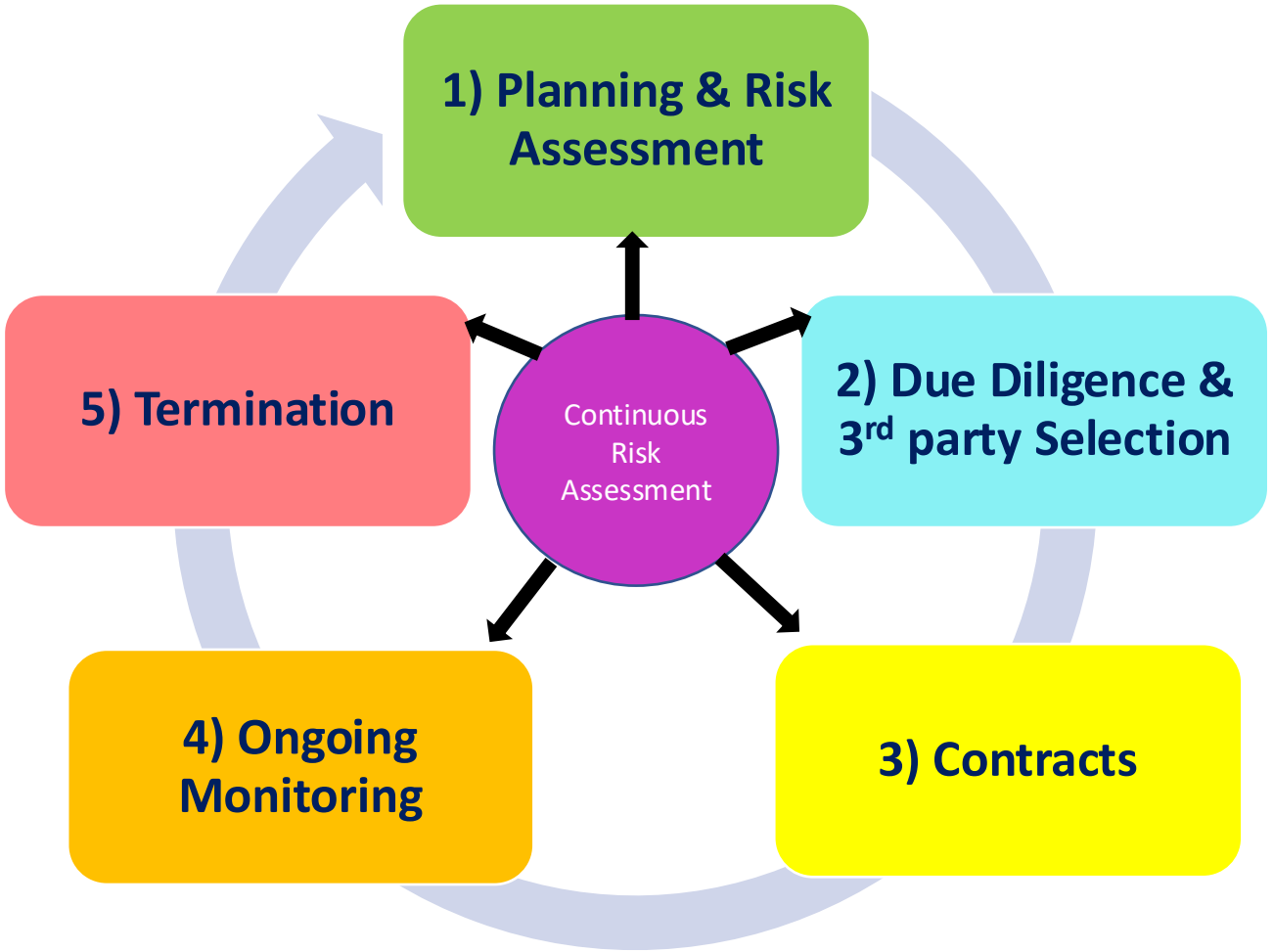
5) Terminations – Why?

- 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



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

Next Steps

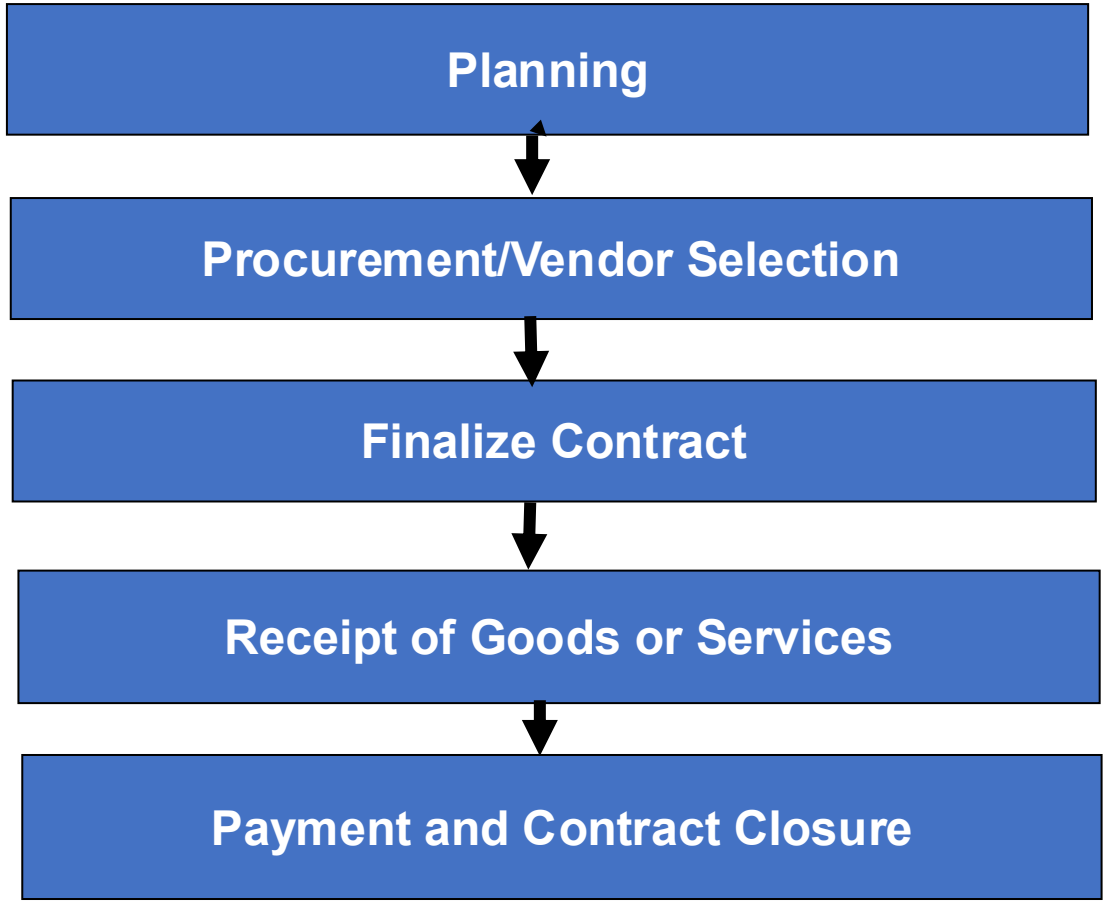
- Identify the third-parties in your influence
- Assess the risks

  With your team!
  - What adverse situations could occur?
  - What would the impact be?
  - What's the likelihood that could occur?
- Ensure there are mitigation strategies in place
- Monitor, monitor, monitor

Be a Risk Champion

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Contracting Process



Planning

- Need justification
- Prepare statement of work
- Evaluate procurement options
- Assemble “team” (e.g., unit, procurement services, legal, business & finance, IT, HR)
- Evaluate compliance requirements

Procurement/Vendor Selection

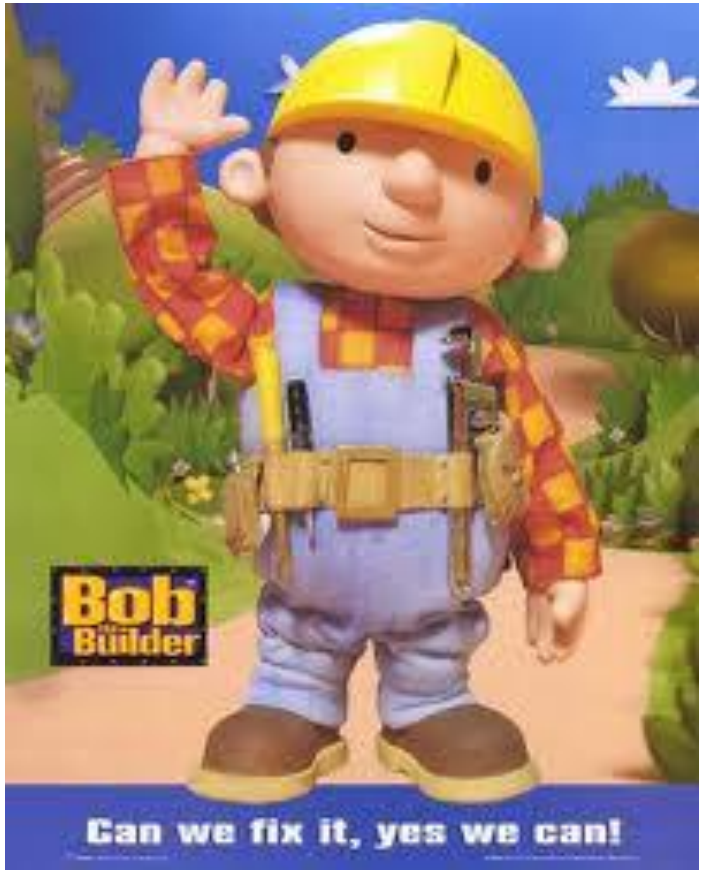
- Initiate procurement process
- Prepare contract request forms
- Ensure fair bidding process
- Ensure no conflict of interest
- Determine contract type

Types of Professional Services Contracts

Fixed Price

- Agreed-upon price for services
- Contractor has majority of risk for cost overruns
- Intent to motivate contractors to innovate processes for cost savings
- Vigilance required to ensure task completion as specified
- Well defined specs are key to avoid changes to scope

How to view contractors…

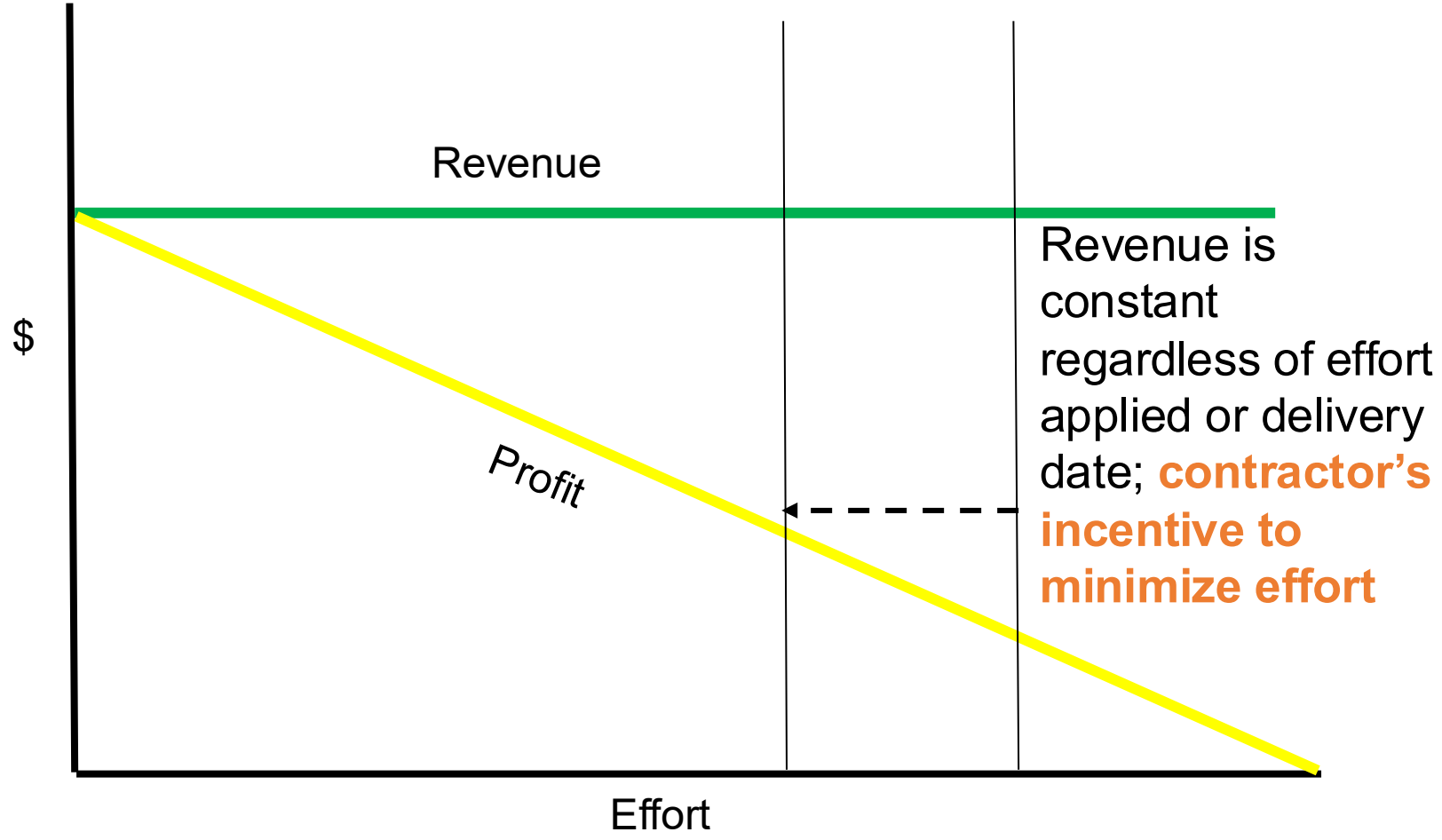


or

How are contractors viewed at your institution?

1) Trusted and treated like they are part of the team
2) Treated as outsiders who are just trying to milk the institution
3) Seen as valuable resources but without loyalty to the institution
4) We have contractors?

Contractor's View of Fixed Price

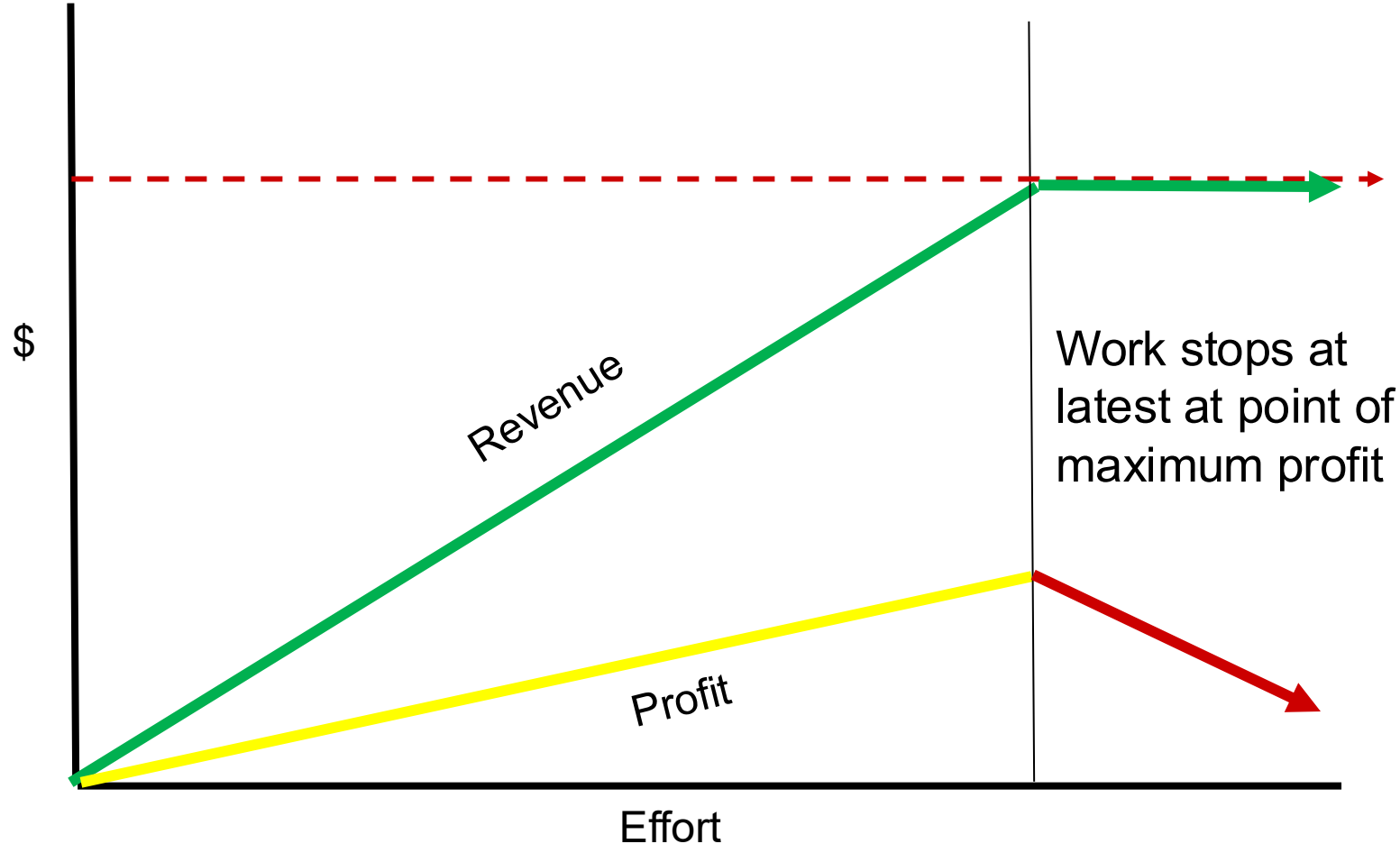


Types of Professional Services Contracts

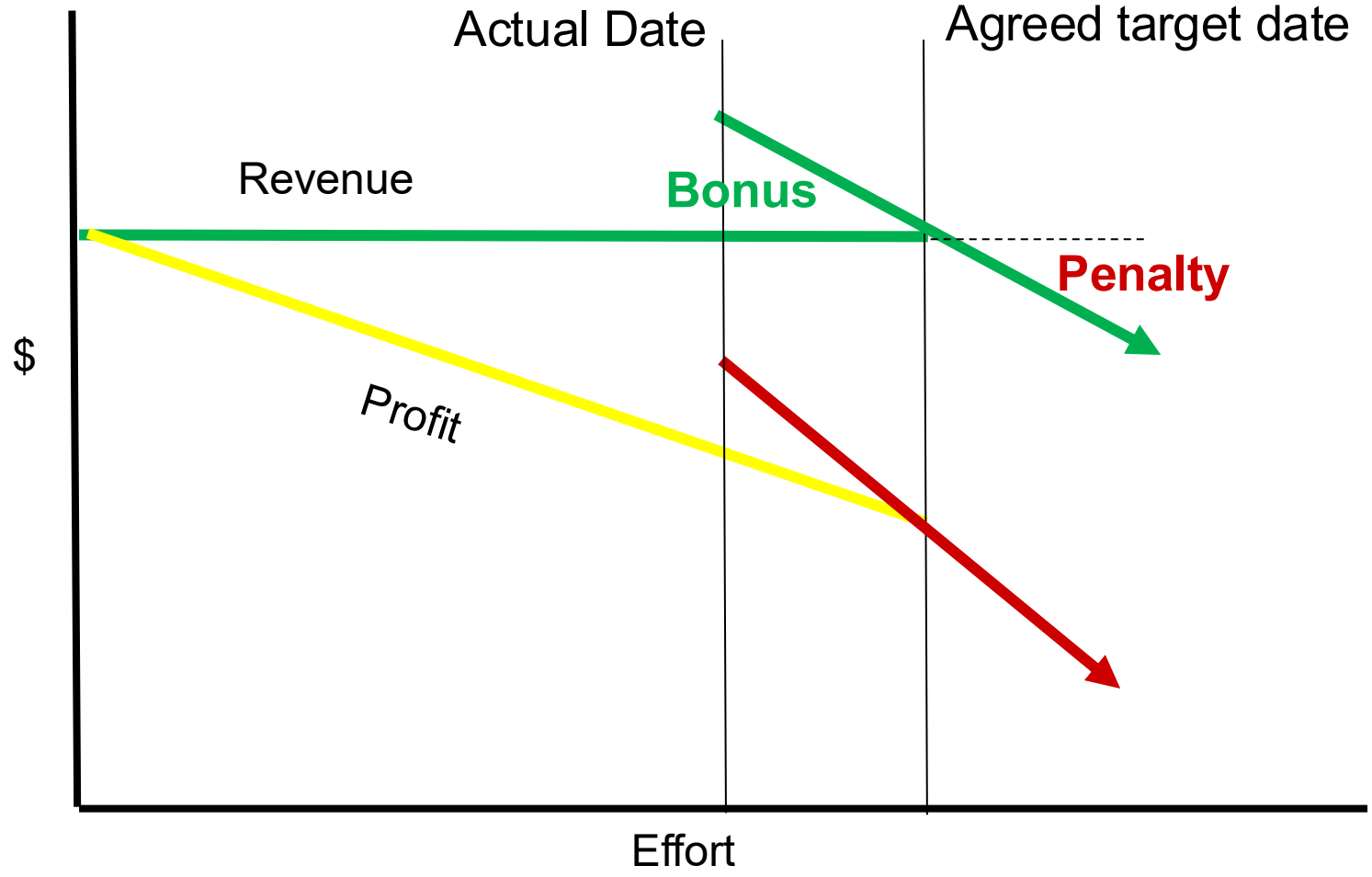
Cost Reimbursement with Guaranteed Maximum Price (GMP)

- Contractor bills for incurred costs up to ceiling
- Best used with incentives such as awards for coming in under budget, ahead of schedule, etc.

Contractor's View of Cost Plus GMP



Bonus / Penalty Clauses



Does your institution use bonus incentives?

1) Yes
2) No
3) No clue
4) What are you talking about? I zoned out after the second graph

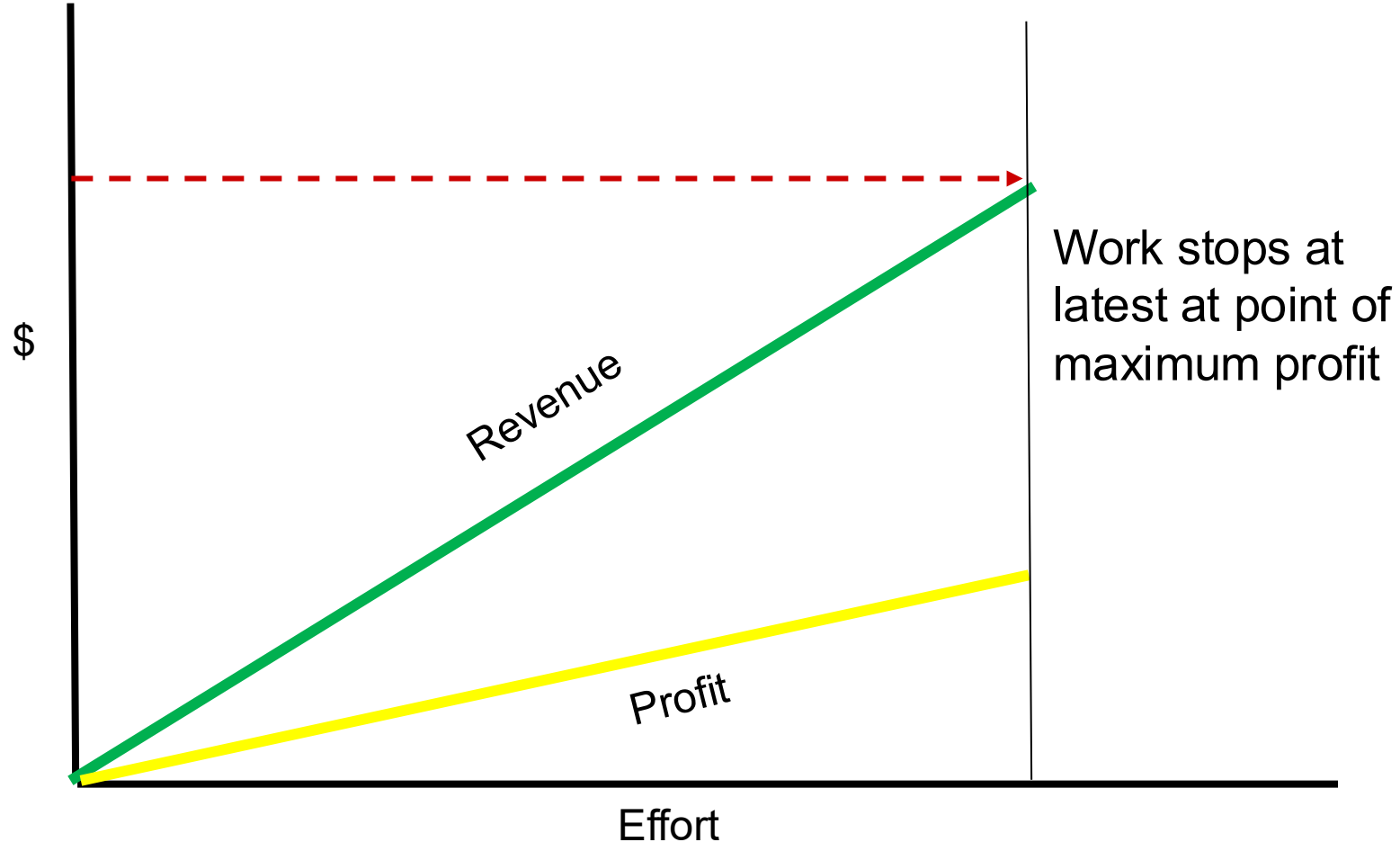
Does your institution use bonus incentives?

Types of Professional Services Contracts

Time and Material

- Usually focused on direct labor hours;
- Used when reasonable estimate not easily determined; provides no incentive to contractor to control expenses, therefore requires more oversight

Contractor's View of T&M



Types of Professional Services Contracts

Indefinite Delivery

- Used when not able to define desired amount of service or delivery date of service
- Relies on additional task orders to be issued at a later date to specify services needed

Most of the contracts at my institution are:

1) Fixed Price
2) Cost Reimbursement with Guaranteed Maximum Price (GMP)
3) Time and Material
4) Indefinite Delivery
5) No clue

Finalize Contract

- Evaluation of proposals (contract review committee)
- Justification of supplier (verify bidding compliance)
- Finalize terms and conditions (T&C's)
- Clarify milestones and deliverables
- Review financial considerations
- Determine how contract will be managed and tracked

Receipt of Goods or Services

- Quality assessment
- Ensuring T&C's have been met
- Ongoing contract management

Payment and Contract Closure

- Review of invoice
- Review of deliverables
- Ensure no outstanding issues
- Accounts Payable process
- Final payments to supplier
- Release commitments
- Close file

Key to Effective Contract Management

- **Collaboration**

- **Centralization**

- **Standardization**

Recommended Resources

- National Contract Management Association (NCMA)
- “Effectively Managing Professional Service Contracts” – IBM Center for The Business of Government
- “10 Contracts for your Next Agile Software Project” – Peter Stevens

Best Practices

1) Clearly define expectations of success for the contract

- What are the goals?
- How will we know if it is successful?
- Who will make that determination?

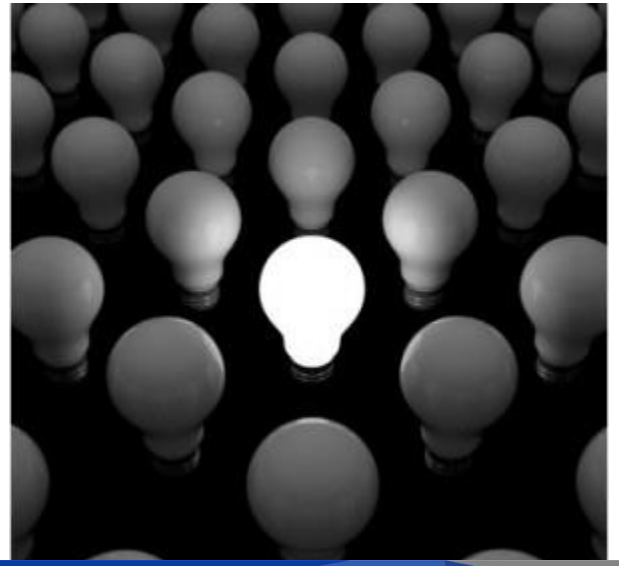
Best Practices

2) Use a contracting approach that supports a "partnership" with the contractor

Best Practices

3) Define and follow a fair bidding and awarding process

- Centralizing and standardizing as much as feasible



Best Practices

4) Provide orientation for contractors

- Clarify **performance expectations**, reporting, briefings, etc.
- **Key people** within the organization
- **Politics and culture** (how things "really work," best way to influence people)
- **Language** (terminology, jargon, unique acronyms, abbreviations, etc.)
- **Organizational goals & values** (how is this project aligned?)
- **History** (Particular traditions followed? Have similar projects in the past failed?)

Best Practices

5) Develop integrated project team to enhance productivity and ability to adapt to changes

- Comprised of disparate individuals
- Establish shared goals of high-quality work at reasonable cost

A take-away from this is that:

1) We need to develop more of a team approach to managing contracts
2) There needs to be clear accountability for who is monitoring contractors
3) I’m going to quit my job and become a contractor
4) I’m going to quit my job and become an auditor

Best Practices

6) Clearly define roles and expectations for university staff and contractor staff

- Who is responsible for key decisions?
- Who organizes meetings?
- Who decides when issues need to be escalated?
- Where will contractor be located and working?

Best Practices

7) Actively manage staff and contractor turnover

- Developing and retaining strong team is critical

Best Practices

8) Motivate and reward contractors to increase commitment and decrease turnover

- Find ways to acknowledge and reward efforts
- Simple “thank you” notes go a long way

Best Practices

9) Regularly monitor performance and provide feedback

- Utilize performance assessments (don't wait until issues are "in the RED" before they are addressed)
- Scorecard system for both contractor AND university

Best Practices

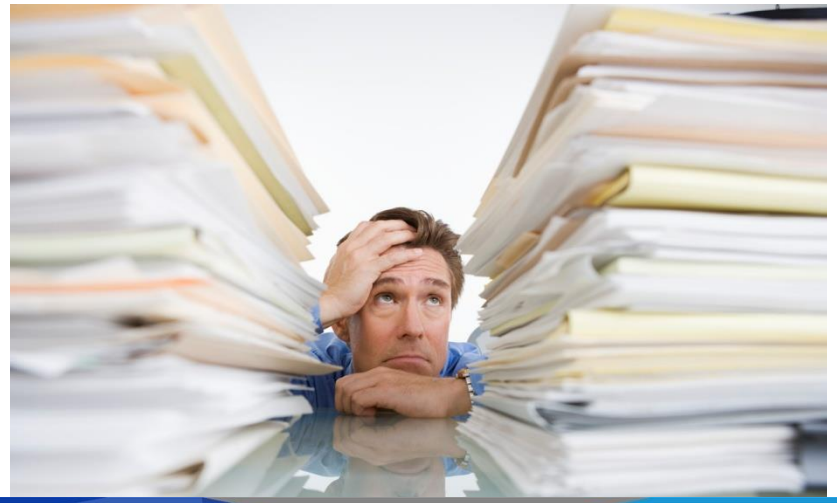
10) Establish clear communication processes among project team members

- Documents clearly communicate what is expected, how results will be measured, what will be rewarded

Best Practices

11) Use knowledge management practices to enhance project performance in spite of short-term costs

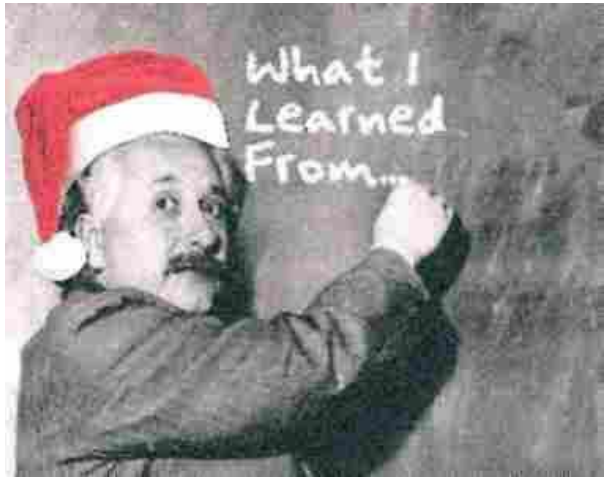
- What happens to intellectual property and knowledge when project is completed or project management changes?
- Can be costly to document but may be critical to sustainability and future success



Best Practices

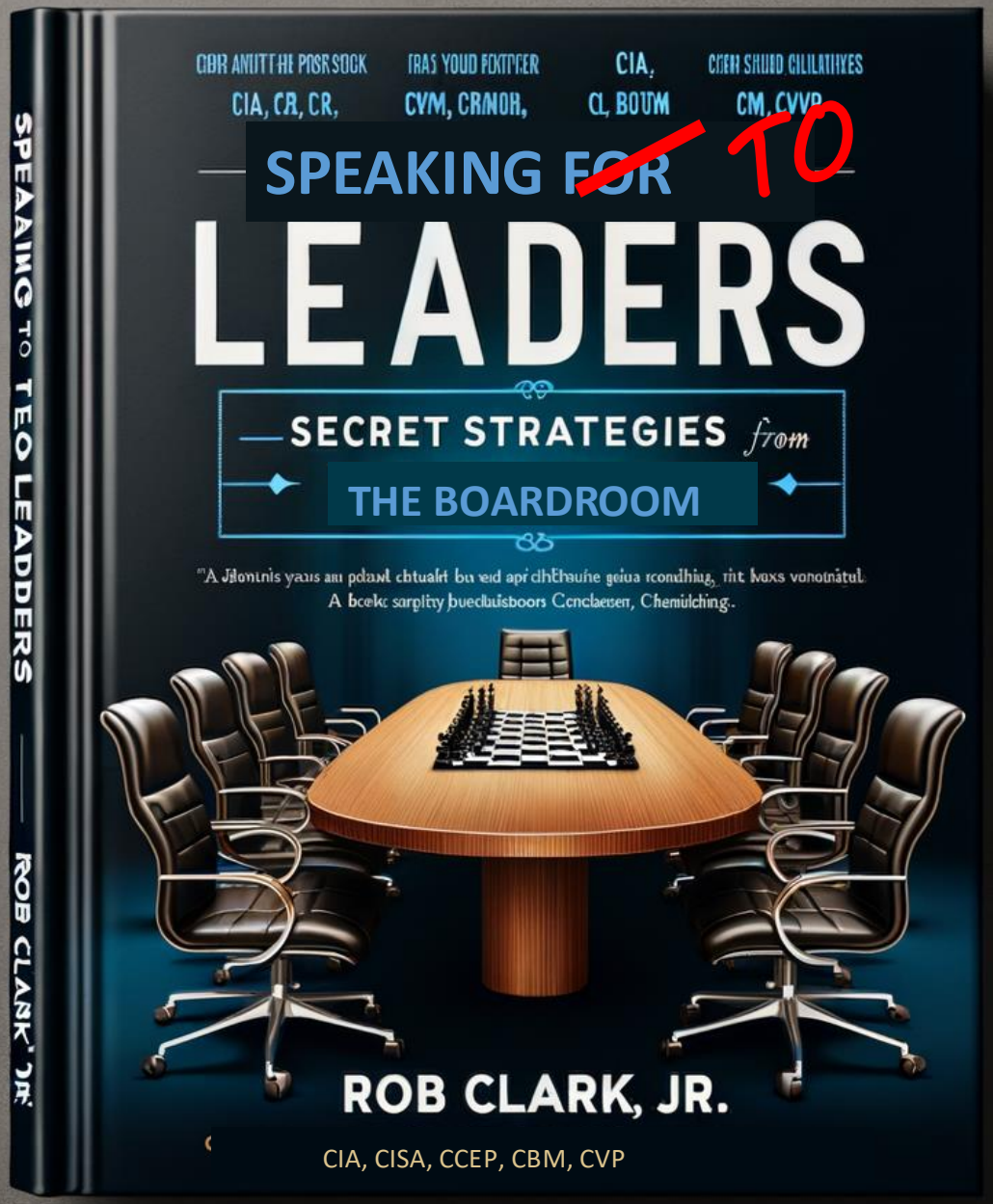
12) Use after action reports to help managers apply lessons learned to other projects and contexts

- Capture “lessons learned”
- Modify procedures to benefit future endeavors and improve effectiveness and efficiency of project and contract management



12) Use after action reports to help managers apply lessons learned to other projects and contexts (cont.)

- Successful contract management is more than just reading the fine print…
- It's making sure resources are effectively and efficiently utilized
- It's a "shared responsibility"
- So, what is YOUR part in that?



What are the next steps for YOU?

1) Evaluate the processes to manage third-parties to identify risks
2) Reach out to Purchasing and Legal to find out how many third-parties you have
3) Talk with IT about implementing an IT Governance policy and council
4) 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

CPE Credit Code

RobClarkSpeaking@gmail.com
770.815.7922
linkedin.com/in/robclarkjr/
www.RobClarkJr.com