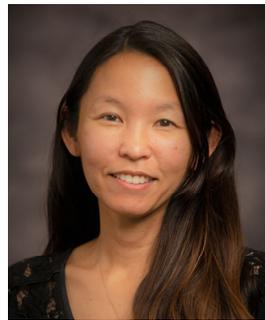




- Don't forget to connect with us on social media!



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



ACUA Virtual Learning Volunteer
Jonathan G. Stadig, CIA, CRMA
Senior Auditor
University of Massachusetts



Risk Management & Risk Resilience

January 26th, 2023



Here with you today...



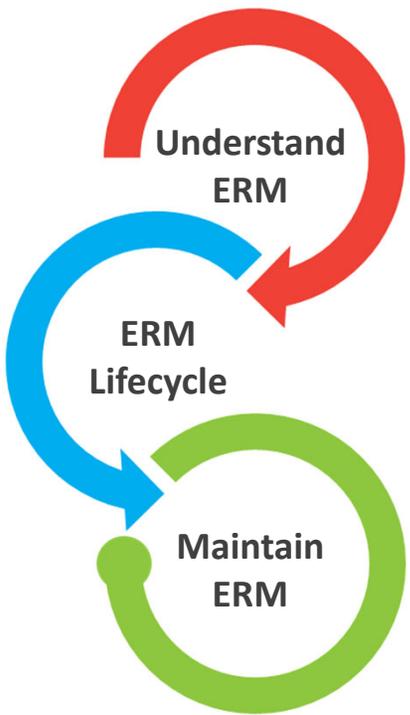
Tina Griffiths
Managing Director
Deloitte & Touche LLP



Jake Braunsdorf
Senior Manager
Deloitte & Touche LLP



Objectives



Articulate the value of Enterprise Risk Management (ERM) programs and how they support risk-informed decision making

Identify the various phases of the ERM lifecycle and the value derived from each phase

Evaluate various leading practices in establishing and/or maintaining ERM programs for use in their institution



Polling Question #1

Does your institution have an ERM program:

- a. Yes
- b. Yes, but the program could be strengthened
- c. No
- d. I'm not sure



Polling Question #2

If your institution has an ERM program, under which department does it report [select all that apply]?

- a. The same leader oversees both Internal Audit and ERM
- b. Chief Risk Officer
- c. Directly reports to Finance
- d. Directly reports to the President and/or Board
- e. Office of General Counsel
- f. Other
- g. We do not have an ERM program



Contents

- 34 The case for Enterprise Risk Management (ERM)
- 35 The ERM lifecycle – process and value
- 36 Leading practices for establishing and maintaining an ERM program
- 37 Q&A



The case for ERM



The case for ERM

ERM is a set of practices that **can help higher education institutions address the full spectrum of the organization's risks**, as well as challenges and opportunities. There are numerous benefits ERM can provide higher education institutions, especially as the institution matures and breaks down organizational silos to enable a true enterprise-wide view of risks.

ERM helps higher education institutions by...

1

focusing on higher education institution's mission and strategic priorities.

2

helping protect higher education institution's brand and reputation.

3

improving strategic decision-making and resource allocation.

4

enhancing a risk-aware culture as risks are openly communicated.

5

providing standardized tools to use in managing risk and sharing risk information.



The changing landscape of higher education

The higher education sector is experiencing change at an accelerating rate, creating opportunities and a growing array of risks that can quickly derail institutions' strategies.

Driving Forces of Risk

<p>Hyper Transparency</p> <p>Institutional conduct is increasingly visible and scrutinized, magnified by instantaneous communication and availability of information.</p>	<p>Evolving Stakeholder Demands</p> <p>Assertive views on strategic and operational investment decisions and intolerance for underperformance.</p>	<p>Regulatory Intensity</p> <p>Increased regulatory demands and practical constraints to strategy.</p>	<p>Information Intensity</p> <p>Big Data is enabling stronger analytical capabilities and creating a need for greater information protection.</p>
--	---	---	--

Common Higher Education Risk Areas

 <p>ENROLLMENT SUPPLY RISKS:</p> <ul style="list-style-type: none"> • International student enrollment • Recruiting and strategic enrollment management • Immigration and federal policies • Growing economic markets • Market demand • Rising student debt 	 <p>BUSINESS MODEL RISKS:</p> <ul style="list-style-type: none"> • Tuition dependency • Education delivery mix • Endowment returns • Recruiting and targeting • Heightened cash monitoring 	 <p>COMPLIANCE RISKS:</p> <ul style="list-style-type: none"> • Federal, state, and local regulations • Research expenditures • Fraud 	 <p>REPUTATION RISKS:</p> <ul style="list-style-type: none"> • Brand management • Campus safety • Student activism • Declining public sentiment 	 <p>OPERATING MODEL RISKS:</p> <ul style="list-style-type: none"> • Operational efficiency • Third-party vendors • Accreditation • Facilities and asset management • Business continuity and crisis management • Talent management • Cybersecurity
---	---	---	---	---



Drivers for risk management in higher education

Institutions should be re-thinking how they look at risk. While risk management has historically been confined to specific domains (e.g., compliance, internal audit, safety, insurance) and often managed in siloes, institutions today are realizing their risk portfolio is inherently interconnected.



Rapid changes in institutional business model and enrollment supply (e.g., education delivery mix, recruiting, market demand, and rising student debt)



Higher prevalence of crises and reputation-damaging incidents (e.g., admissions and enrollment scandals, Title IX)



Increased board interest in establishing robust and proactive comprehensive risk programs



Provides institution the ability to make **risk-based decisions** on **data driven measurements**

Interested Parties

- Chief Risk Officers
- Director of Risk Management
- Director of Risk & Compliance
- VP of Finance
- Board of Directors
- Provosts
- Deans



Polling Question #3

Which of the following is NOT a driving force for the need to have a risk management program in higher education:

- a. Admissions scandals
- b. Evolving stakeholder demands
- c. Lack of market volatility
- d. Regulatory intensity
- e. Rapid changes in institutional business model and enrollment supply



The ERM lifecycle – process and value



Polling Question #4

What are the five stages of the ERM lifecycle?:

- a. Identify, evaluate, prioritize, respond, monitor & report
- b. Identify, assess, purpose, respond, monitor & report
- c. Identify, assess, prioritize, respond, monitor & report
- d. Identify, assess, prioritize, reply, monitor & report



The ERM lifecycle

The ERM lifecycle is a repeatable process to identify and manage risks.



Phase

Identify: Identify and categorize risks that impact the achievement of strategic goals and objectives

Assess: Apply risk rating criteria to evaluate overall exposure to the identified risks

Prioritize: Determine the most critical risks

Respond: Develop response to accept, avoid, reduce, transfer, or exploit risk

Monitor: Provide timely and relevant updates to leadership on risk information



Risk identification – process and value

During Risk Identification, stakeholders work together to identify and define the risks that impact the achievement of a higher education institution's strategic goals and objectives.

Steps that can be taken during risk identification

- 1 Risks are gathered through cross-department insights and perspective through a combination of interviews and risks surveys to understand the risks and challenges that they face.
- 2 The risks that are described by leadership are articulated into "if/then" statements to describes both the risks and consequences higher education institutions faces to drive assessment and action.
- 3 The risks statements are validated by stakeholders to confirm that they accurately describes the risk higher education institutions face.
- 4 A risk register is developed to capture and document the universe of risks identified by stakeholders to facilitate assessment, prioritization, and monitoring.

VALUE: Risk identification helps management think through current or potential risks to the mission and strategic goals of higher education institutions and helps them identify common risks, challenges, and causes across the department.

Risk identification tools

The image displays four distinct tools used in risk identification:

- Risk Lexicon:** A screenshot of a table with columns for 'Term' and 'Definition', providing a structured list of risk-related terms and their meanings.
- Risk Taxonomy:** A screenshot of a complex web-based interface with multiple tabs and a central grid, likely used for organizing and categorizing risks.
- Risk Surveys/Workshops:** A screenshot showing several line graphs and data visualizations, representing the results of surveys or workshop discussions.
- Risk Register:** A screenshot of a data table or spreadsheet, used for tracking and documenting identified risks over time.



Risk identification | What types of risk do you consider?

The desired method for identifying risks depends on its type. If the risk is unknown or emerging, the advantageous way to identify it may be different than the most common method to identify known risks. Only looking retrospectively may result in certain risks being overlooked.

	Unknowns	Emerging	Known Unmanaged	Known Managed
Description	<ul style="list-style-type: none"> • What if's • Requires creativity above all else • "Unknown unknowns" 	<ul style="list-style-type: none"> • Small/low frequency events and changes to the internal/external environment, but potential high impact if frequency grows • Enterprise impacts still difficult to imagine • No controls in place, limited monitoring • "Known unknowns" 	<ul style="list-style-type: none"> • More likely to materialize • Stronger signals • No response plan in place 	<ul style="list-style-type: none"> • Mitigation in place • Accountability is assigned • Can apply risk appetite level
Identification Method	<ul style="list-style-type: none"> • Black Swans – low probability, high impact scenarios • War gaming • Define early signals and tipping points 	<ul style="list-style-type: none"> • Monitor "what if's": signs and tipping points; thresholds beyond which escalation is needed • Analysis to confirm it is an enterprise risk • Risks that materialized at other agencies, but not Agency • Risk sensing 	<ul style="list-style-type: none"> • Surveys • Executive interviews • Workshops 	<ul style="list-style-type: none"> • Surveys • Executive interviews • Workshops
Considerations	<ul style="list-style-type: none"> • Some will leak through and emerge later 	<ul style="list-style-type: none"> • Sooner can detect, more you'll be able to manage • Less time on assessment, more time on monitoring 		<ul style="list-style-type: none"> • Focus attention on effectiveness of mitigation, KRI monitoring



Risk Assessment | Risk Taxonomy

A risk taxonomy is a comprehensive classification scheme of risk categories and subcategories to enable consistent identification and categorization of risk. The taxonomy below is a broad representation of a risk taxonomy at a higher education institution, but each institution is unique and will vary in both format and risks.

Administration	Strategy	Academic	Operational Model	Compliance	Student Experience
Cybersecurity and Privacy					
Reputation					
Financial Management	Business Model	Faculty Management	Third-Party Vendors	Federal Regulations	Student Organizations
Human Resources	Enrollment Supply	Accreditation	Business Continuity	State & Local Regulations	Athletics
Information Technology	State Appropriations	Curriculum	Crisis Management	Research Expenditures	Student Housing
Procurement	External Factors		System Coordination	Fraud	Student Well Being
Legal	Campus Development		Campus & Physical Safety		Student Activism
	Continued Growth & Revenue Streams		Facilities & Asset Management		

VALUE: A taxonomy can help your teams to better identify and categorize risks encountered in day-to-day operations by providing a comprehensive break-down of risk categories.



Risk Assessment | Process and Value

During Risk Assessment, stakeholders score each of the risks identified by using a defined methodology to evaluate the impact and likelihood of the risk occurring in order to assess the criticality of each risk.

Steps that can be taken during risk identification

- 1 Each risk is assessed for its potential impact, in consideration of one or more potential categories and interdependencies. In addition, each risk is assessed for likelihood of occurrence.
- 2 The risk scores are plotted on a heat map which enables the stakeholders to conduct an apples-to-apples comparison and understand the relative importance of risks to one another.
- 3 All risk scores are recorded in the Risk Register, including any additional relevant information provided as a result of the assessment to facilitate further review and dialogue. Typically, a risk taxonomy is developed to aid in the organization and communication of risks.

Risk Impact and Likelihood Scales

		Impact Scales				
Criteria Category		1 - Insignificant	2 - Minor	3 - Moderate	4 - Significant	5 - Critical
Administration		Impacts to the institutions ability to successfully conduct its administrative activities (i.e., Financial Management, HR, Procurement, Information Technology, Legal).				
Strategy		Impacts to the institutions ability to achieve its strategic goals and objectives.				
Academic		Impacts to the institutions ability to achieve its academic mission.				
Operational Model		Impacts to the institutions internal processes, capabilities, and systems.				
Compliance		Impacts to the institutions ability to comply with a growing array of state, local, federal, and private regulations.				
Student Experience		Impacts to the institutions ability to provide an engaging student experience.				

Likelihood Scales				
1 - Very Unlikely	2 - Unlikely	3 - Possible	4 - Likely	5 - Very Likely
The event may occur only in exceptional circumstances.	The event could occur in uncommon circumstances.	The event could occur in common circumstances.	The event could occur in relatively common circumstances.	The event is expected to occur in most circumstances.

VALUE: Risk assessment is critical to understanding the interdependencies impacting each risk; and how serious the consequences of risks would be if they were to materialize in the absence of any mitigating controls and practices. Through risk assessment, **stakeholders can think through the criticality of their risk** in relation to all other risks. This step is critical in order to prioritize the key risks affecting higher education institutions.



Risk Prioritization | Process and Value

During Risk Prioritization, stakeholders further evaluate their ranked risks based on a qualitative assessment of which are most important to achieving their strategic goals and objectives.

Steps that can be taken during risk prioritization

- 1 Risks that are similar across offices are identified for potential consolidation. Risk consolidation enables an understanding of risks affecting multiple offices across the department and might need a more immediate response.
- 2 Leaders share their insights and perspectives on each risk to further refine how they think about their risks, identify common drivers between risks, and—finally—prioritize the risks that matter most.
- 3 Leadership participates in a facilitated workshop to discuss current risk management activities for the prioritized risks, and whether what was being done was sufficient to manage the risk to an acceptable level.

Illustrative Risk Tier Definitions

	TIER 1	TIER 2	TIER 3
DESCRIPTION	<ul style="list-style-type: none"> ➤ May have a significant effect on its ability to perform core business functions ➤ Based on current risk response efforts, institution is not currently prepared to address or anticipate the risk 	<ul style="list-style-type: none"> ➤ May have a moderately disruptive effect on its ability to perform core business functions ➤ May have some controls in place to address this risk, but effectiveness is uncertain/unproven 	<ul style="list-style-type: none"> ➤ May cause routine, minor disruption to core business functions ➤ May have experienced or addressed these risks in the past
AVERAGE TOTAL RISK <i>Likelihood * Impact</i>	<i>Total Risk Score > 15</i>	<i>7 < Total Risk Score ≤ 15</i>	<i>Total Risk Score ≤ 7</i>
OTHER CONSIDERATIONS	<ul style="list-style-type: none"> • Could result in delays to institutional priorities • Consider how urgent the risk is (i.e., will impact or likelihood decline in time?) • Requires significantly more time, funding, or staff to manage this risk • This risk is not currently being managed effectively, and/or requires extensive coordination with others • No advance warning signs or indicators 	<ul style="list-style-type: none"> • Stakeholders and management have some awareness of this risk • Will this risk be impacted by time? • Requires a modest amount of additional time, funding, or staff to manage this risk with some external coordination required • Could do more to manage this risk • There is limited advance warning 	<ul style="list-style-type: none"> • Risk is understood and anticipated by stakeholders • The impact / likelihood of the risk changes over time • Requires significantly less time, funding, or staff to manage this risk effectively • Currently, this risk is managed effectively • Ability to predict/anticipate these risks

VALUE: Risk scores from the assessment phase must be discussed and broadly considered by gaining a plethora of different perspectives, including leadership and institutional priorities. Through prioritization, **management establishes department-wide organizational consensus on the risks that are most important to achieving the strategic goals and objectives of higher education institutions**, which help them identify where to focus resources.



Risk Response | Process and Value

Risk response is the process of developing strategic options to address risks that impact an institution's goals and objectives. Risk response strategies are used to produce a range of response options to bring a risk to within acceptable risk appetite, in consideration of optimal cost-benefit effectiveness.

Steps that can be taken during risk response

- 1 Discussions are also held to discuss the range of risk response strategy options for managing each risk (as depicted on the right).
- 2 Also included as part of the discussion, are various additional tactical activities that could be employed to further manage the risk and the various cost-benefits.

Risk Response Strategy Options

Exploit	<i>Is the higher education institution willing to increase the risk it accepts for the pursuit of opportunities?</i>
Accept or Monitor	<i>Can the higher education institution accept the risk without taking further action?</i>
Share or Transfer	<i>Can the higher education institution share or transfer ownership of the risk to other entities to support risk treatment options?</i>
Avoid	<i>Can the higher education institution stop doing the activity causing the risk?</i>
Mitigate	<i>Can the higher education institutions reduce its vulnerability to, likelihood of, or impact of the risk?</i>

VALUE: Management is able to identify and pinpoint the range of risk management activities that they are already doing to manage their Tier 1 risks and discuss whether additional activities are needed.

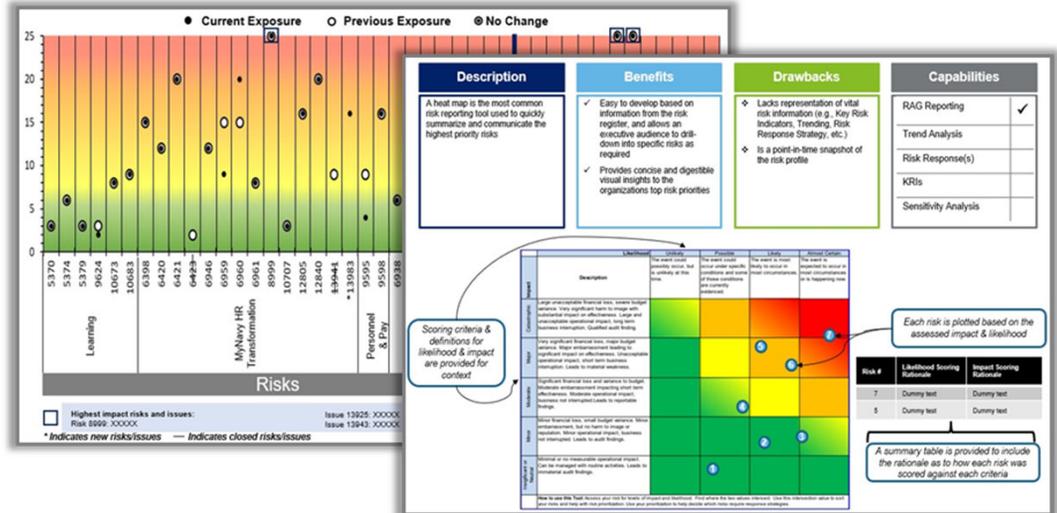
Monitor and Report | Process and Value

Risk should always be tracked in a central location.

Steps that can be taken during risk reporting

1

Leveraging the risk assessment discussions and documents, a heat map (as depicted on the right) is developed to help leadership **understand the severity of risks at a glance** and make decisions on which risks might need additional attention/resourcing.



VALUE: The images above show potential ways to display and report risk information in a centralized location.



Leading Practices for Establishing and Maintaining an ERM Program



Leading Practices for Establishing and Maintaining ERM Program | Enterprise Risk Committee (ERC)

An ERC is part of the larger risk management program capabilities within an organization. There are various stakeholder groups within the program, identified below.



Executive Leadership

The organization's leadership make strategy, policy, and budget decisions based on ERC recommendations.



Enterprise Risk Committee (ERC)

Key leaders assess and prioritize enterprise risks.



ERM Working Groups

Working Groups may include subcommittees to address risks to a specific portfolio, account, or area.



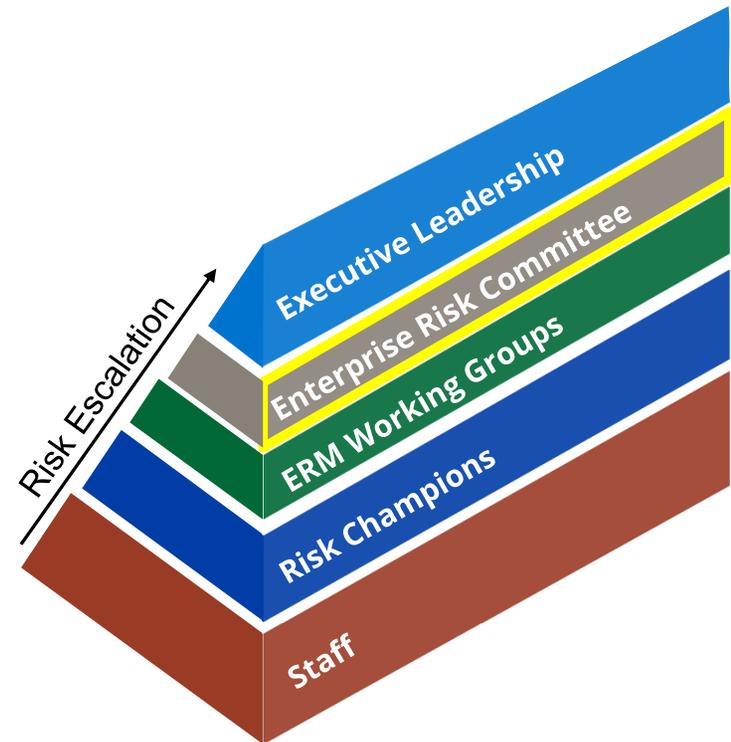
Risk Champions

Risk champions serve as representatives between staff and the ERM working groups.



Staff

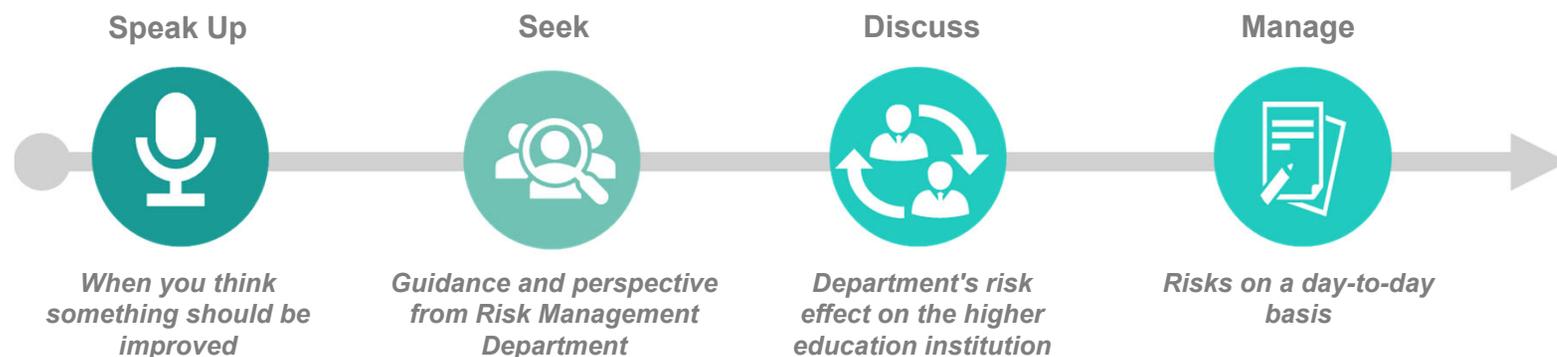
Employees across the organization identify risks.





Leading Practices for Establishing and Maintaining ERM Program | Risk Champions

Risk Champions provide support to ERM by practicing effective risk management and contributing to the maturation of the higher institution's risk management capabilities. Risk Champions engage with the institution's community to integrate ERM principles into their everyday activities. **Effective risk management is a constantly evolving practice.**



Integrate ERM principles into your day-to-day role and support the adoption of ERM.



Leading Practices for Establishing and Maintaining ERM Program | Alignment

Alignment of IA, ERM, and Compliance provides a functional and effective apparatus to identify and respond to risks facing higher education. By aligning these three foundational capabilities, institutions can become risk intelligent.



How do we proactively identify risks?



Are identified controls effective?



What information is required to remain compliant?



Identify, Assess, Mitigate, Respond

- 1 ERM → Compliance: Risk mitigation development strategies/plans feeds Compliance's control enhancement and design efforts
- 2 ERM → IA: Risk Prioritization output feeds IA's work plan that focuses on the highest impact risks to audit

Assure, Advise, Anticipate, Act

- 3 IA → ERM: Provides assurance priority risks are managed effectively, risk management program & internal control framework are operating effectively
- 4 IA → Compliance: informs potential updates and/or modifications to control designs and policies

Design, Assess, Implement, Articulate

- 5 Compliance → IA: Provides reports to IA on compliance program activities that help inform IA's audit plan and scope
- 6 Compliance → ERM: Control monitoring output informs the risk register by indicating processes or business units with higher levels of noncompliance

A risk intelligent culture supports the active identification, monitoring, assessment, and ability to respond to risks in a consistent and transparent manner. The diagram provides our perspective on the components of a risk intelligent institution.



Protections Around Documenting Risk Information

Risk conversations are often **confidential and for management decision making purposes only**. They are also considered an **attorney work product and fall under attorney-client privilege** when they are performed at the "direction of the attorney"



While this is a **legal concept**, it's the best way to protect against risk information being utilized in discovery



Attorney does not need to be present for each discussion, but should be involved in risk assessment process

This allows for **three approaches** to documenting risk information



Transparent: everything is shared and 100% transparent and tends to be utilized to air major issues



Protected: documents are labeled "**confidential and for management decision making purposes only**" protecting them from **FOIA and related public inquiry OR** attorney is involved in all discussion with all risk information considered privileged and typically utilized to make stakeholders more comfortable



Hybrid: for any topic you want to keep privileged and confidential, you have an attorney present, while everything else is open and transparent



Leading Practices for Working With Your OGC

OGC typically struggles with identifying who owns risks within an institution, and as a result, do not know who to engage with.

CULTIVATING A MUTUALLY BENEFICIAL RELATIONSHIP WITH OGC

BEST PRACTICE 1:

Hold initial meeting with OGC to socialize ERM initiative.

Set a **regular cadence of meetings** with OGC and keep them apprised of any risks or challenges you are facing to get a legal lens on risk

BEST PRACTICE 2:

Check in with OGC whenever you believe you are **interpreting a law or regulation and to share key risk information.**

OPPORTUNITIES FOR ENGAGEMENT WITH OGC IN THE RISK ASSESSMENT PROCESS

RISK

IDENTIFICATION:

An attorney can help determine if "is this really a risk" by putting a **legal lens** on versus what is seen from an operational perspective

RISK MITIGATION:

An attorney can help **strategize what is possible** in terms of response

RISK ASSESSMENT:

An attorney can help with **classifying risk severity** by offering insights into levels of legal exposure



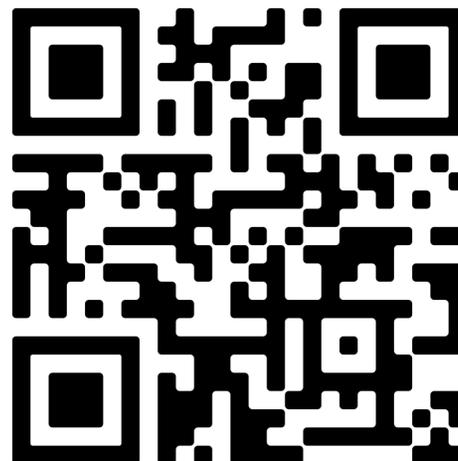
Questions & Answers



QR Codes to LinkedIn



Tina Griffiths
tgriffiths@deloitte.com



Jake Braunsdorf
jbraunsdorf@deloitte.com



This presentation contains general information only and the presenters are not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

The presenters shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.



> **Upcoming ACUA Events**

Webinars

February 23, 2023 – Baker Tilly
Student Well-Being Risk Assessment

Audit Interactive

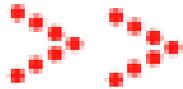
March 26-29, 2023 in Denver, CO
Early bird registration by February 13, 2023



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

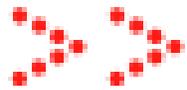


New Kick Starter Available!

Cost Allocation and Recovery

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

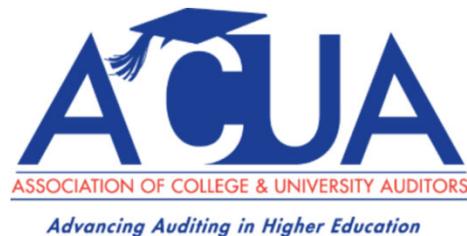




Next Kick Starter Release is February 15th!

Student Athletes Medical Records Privacy

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





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**
March 26 – 29, 2023
Denver, CO
 - 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 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.



**Join us for
our upcoming
webinar.**

