BAKER TILLY

Operation Collaboration:

Leading Practices for Leveraging Common Internal Audit and Compliance Structures at Higher Education Institutions

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.

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

Key learning objectives

- Understand key characteristics, advantages and disadvantages of several IA and Compliance structures
- Implement leading practices for institutional collaboration between IA and Compliance functions
- Apply effective methods for IA and Compliance to coordinate communications with the Board of Trustees and Audit Committee
- Discuss how IA can provide objective assurance and monitoring for the Compliance function

BAKER TILLY

Candor. Insight. Results.

Introduction

Challenges and opportunities for IA and Compliance

Intersection of IA and Compliance

Internal audit

- Concerned with all risks to an institution
- Operates independently of management
- Third line of defense

Cross-functional collaboration results in:

- **Streamlined processes**
- **More efficient use of institutional resources**
- **Simplified, direct lines of communication**
- **More informed decision making**
- **Sound governance and risk management**

Compliance

- Concerned primarily with regulatory risk; more restricted scope than IA
- Ensures compliance with external laws/ regulations and policies
- Second line of defense

BAKER TILLY

Challenges with effectively managing and mitigating risk and compliance continue to grow due to:

- Increased external legal and regulatory requirements and the subsequent risk of non-compliance
- Pressure from the Board due to heightened industry scrutiny resulting from high profile instances of non-compliance
- Limited institutional budgets and resources
- Demand for technical/skilled resources to support ever-changing institutional needs; complex operations

BAKER TILLY

Seven elements of an effective compliance program:

1. Development and distribution of written standards of conduct, as well as written policies and procedures
2. Designating a compliance officer and compliance committee
3. Development and implementation of effective training and education
4. Developing effective lines of communication
5. Responding promptly to detected offenses and developing corrective action
6. Conduct monitoring and auditing
7. Enforcing standards through well-publicized disciplinary guidelines

BAKER TILLY

Risk management – the role of IA and compliance

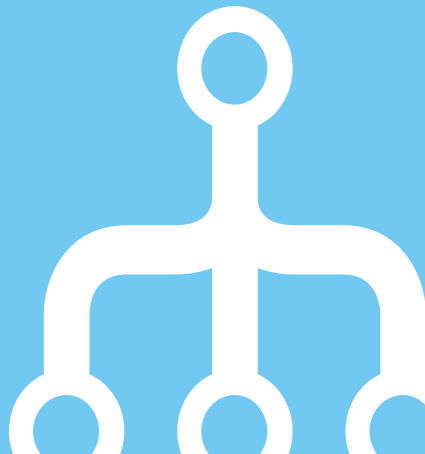
First line	Second line	Third line
		
Risk owners or managers	**Risk control and compliance**	**Risk Assurance**
> Operating management	> Limited independence > Reports to management	> IA > Greater independence > Reports to governing body

BAKER TILLY

Candor. Insight. Results.

Variations in reporting relations

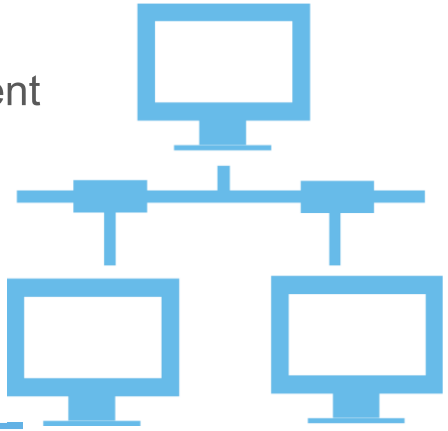
Common organizational structures in higher education



Variations in reporting relations

Examples of IA and Compliance organizational reporting structures include:

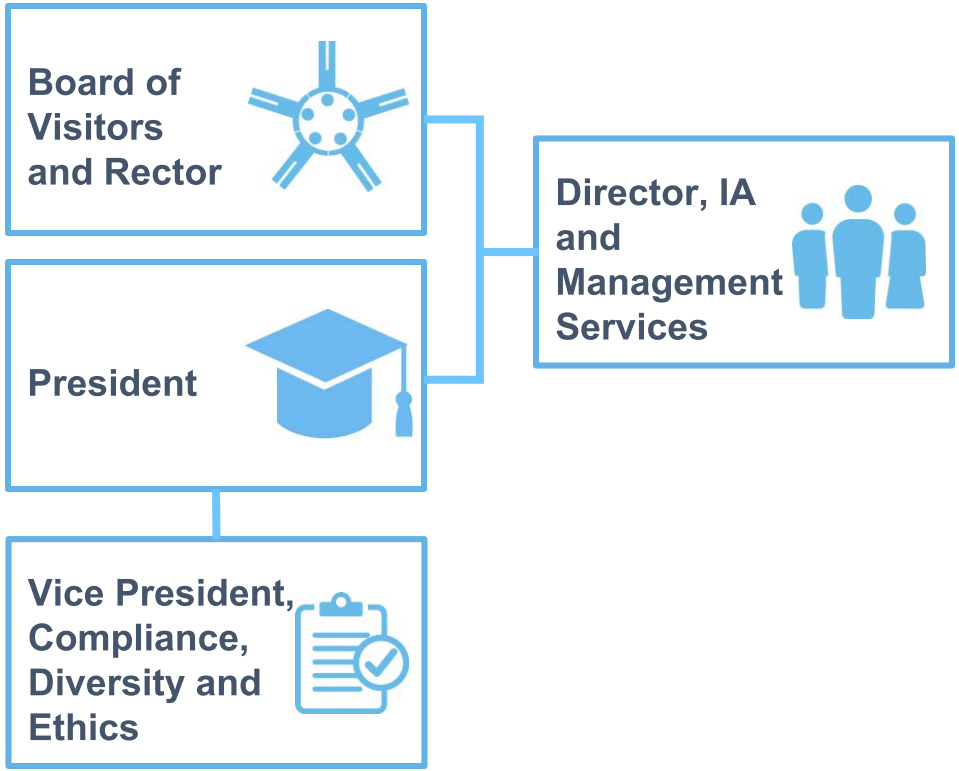
- IA and Compliance are distinct internal departments with separate reporting relationships to Senior Leadership (e.g., Board, President)
- IA and Compliance are placed within the same internal department under the same leader
- Compliance responsibilities are spread across the institution to various functions (e.g., Title IX coordinator)
- Other common IA and/or Compliance organizational reporting structures



Variations in reporting relations

Separate internal departments

- IA and Compliance are distinct institutional departments with separate reporting relationships to Senior Leadership
- Compliance reports directly to the President or some other institutional leader
- IA dually reports to the President and the Board of Visitors and Rector



Separate internal departments

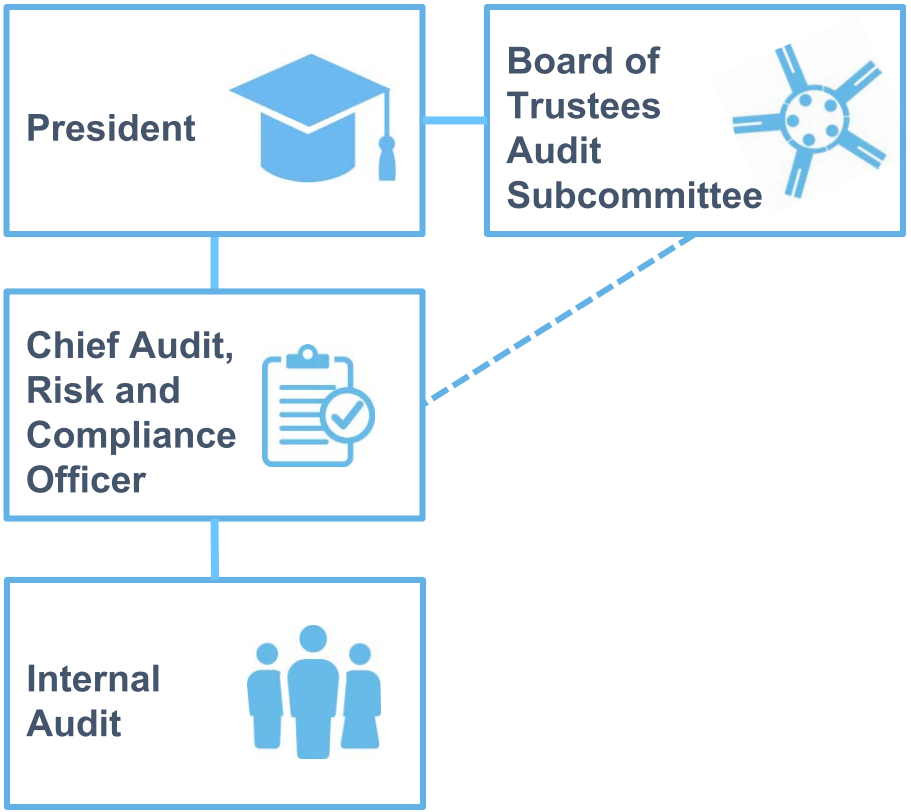
George Mason University Office of Compliance, Diversity and Ethics

- Compliance reports directly to the President
- IA reports separately to the President *and* Board of Visitors
- Multiple lines of reporting reduces the likelihood of critical issues or institutional risk areas “falling through the cracks”
- If necessary, IA can supersede the President and report directly to the Board
- Requirements for success include:
  - Efficient and consistent communication
  - Clear delineation of roles and responsibility
  - Trust

Variations in reporting relations

Single central department

- IA and Compliance are placed within a single institutional department
- Jointly report to the Board of Trustees or other institutional leader(s)
- IA also collaborates with third-party resources/experts



Montgomery College Office of Compliance, Risk and Ethics

- Key areas of responsibilities:
  - Internal audit
  - Regulatory compliance
  - Americans with Disabilities Act (ADA) compliance
  - Title IX compliance
  - Youth protection
  - State ethics reporting
  - Code of ethics
  - Enterprise risk management

BAKER TILLY

Compliance responsibilities spread across the institution to various functions

- Compliance function not formally defined
- Responsibility for individual compliance areas distributed to related internal function
- IA supports compliance assurance by auditing decentralized compliance areas and report findings to the Board

Information privacy

National Collegiate Athletic Association (NCAA)

Human and animal research

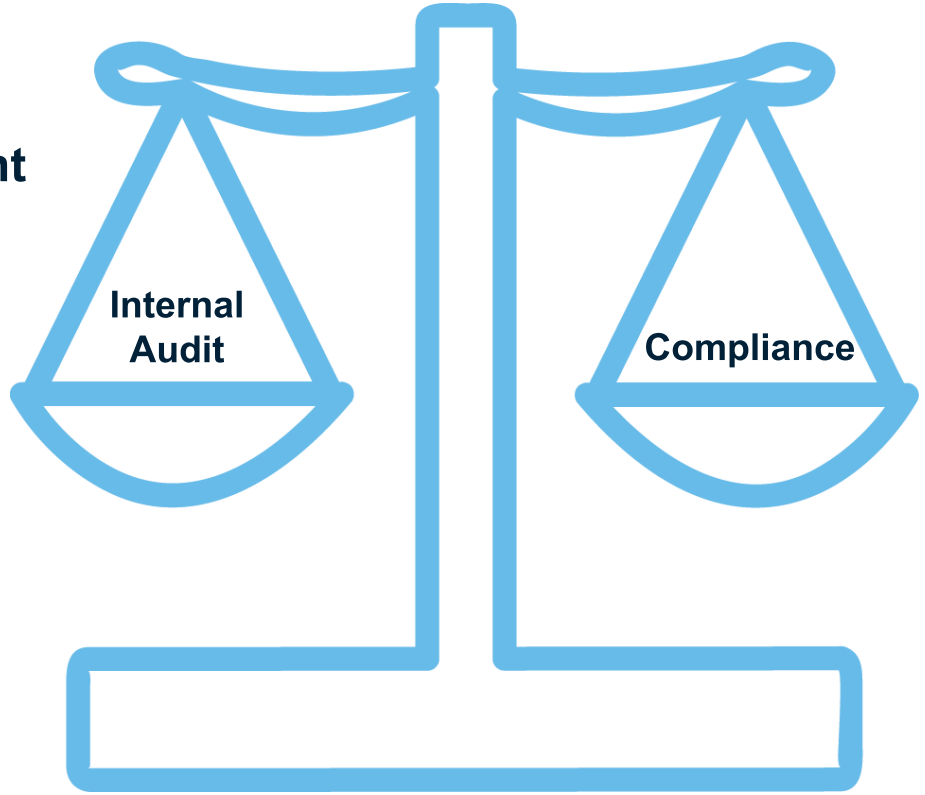
Research conflict of interest process

Title IX coordinator

Variations in reporting relations

Decentralized compliance environment

- IA can work with stakeholders to evaluate emerging risks in the higher education industry
- IA can monitor compliance-related reporting risks for Senior Leadership
- IA can report audit results and findings to the Board in lieu of Compliance

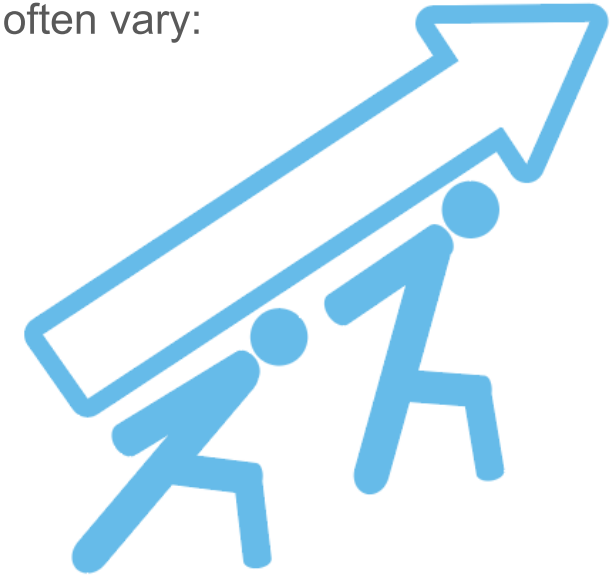


Variations in reporting relations

Other common IA or Compliance organizational reporting structures

IA and Compliance reporting structures often vary:

- Chief Financial Officer
- Provost
- Chancellor
- Board of Trustees
- Other Senior Leadership



BAKER TILLY

Candor. Insight. Results.

Operation collaboration

Collaboration initiatives of leading peer institutions

Operation collaboration

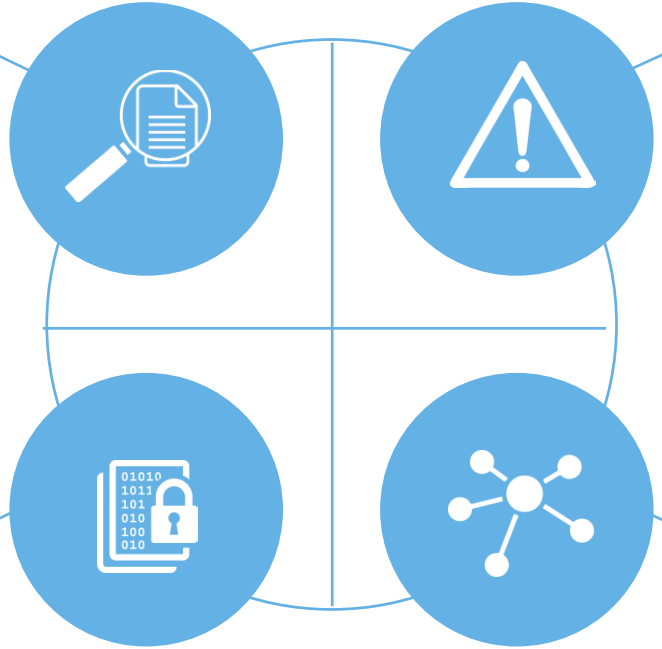
Areas for Collaboration

Risk assessments

Assess and prioritize institutional risk to inform IA of future high-risk audit areas

Audit activities

IA and Compliance audit initiatives



Investigations

Responding to reported breaches of external laws or violations of internal policies

Compliance governance assessments

IA assesses and advises Compliance to achieve sound governance

Developing a common “risk language”

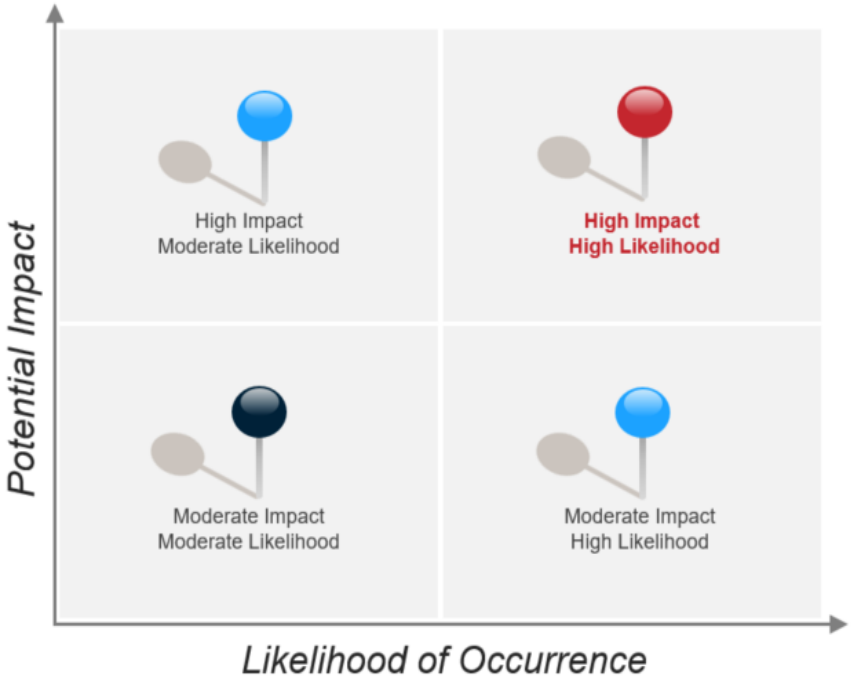
Improves communication between risk manager(s) and Senior Leadership/ the Board

Allows for a more **unified and integrated approach** to managing institutional risk

Assists the Board in **understanding the integral value** of IA and Compliance to the institution

Risk assessments

- Identify emerging regulatory risks that could affect the institution
- Examine current institutional practices and controls for mitigating these risks
- Collaborate to prioritize top risks and discuss the best approach to address those risks going forward



Case study: enterprise risk assessment

- Compliance office engaged IA to perform an enterprise risk assessment and provide an institution-wide coordinated view of risk
- IA and the Compliance office:
  - Identified emerging risks that could affect the institution
  - Examined current institutional practices for mitigating risk
  - Determined the best options for addressing risk going forward
- Compliance office used the enterprise risk assessment results from IA to develop a subsequent, three-year risk-based IA plan

Audit activities

- How IA and Compliance activities fit together
- Industry insights into collaborative initiatives between IA and Compliance
- Example case studies of projects at various institutions with different reporting structures

Case study: export control audit

- IA engaged external subject matter expert (SME) to assist with an audit of Compliance's Export Control Program
- SME collaborated with Compliance to audit and evaluate the adequacy and effectiveness of the institutional policies and processes and compliance with external laws and regulations
- SME audit scope included:
  - Review of policies and procedures; evaluation of internal policy compliance
  - Identification and testing of key controls
  - Walk-throughs of facilities and interviews of key process owners

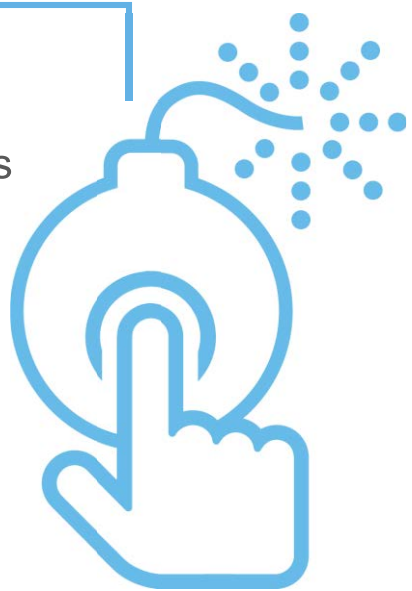
BAKER TILLY

Case study: IT accessibility

- Compliance office developed and implemented policies and procedures to standardize expectations of IT accessibility across the institution and to ensure institutional compliance with federal IT accessibility laws and regulations
- Compliance office engaged IA post-implementation to assess institutional compliance with the IT accessibility policies and procedures and minimize the risk of non-compliance
- IA and Compliance developed a plan for future audits to assess IT accessibility compliance (e.g., IA assurance review to verify accessibility of information on the institution's ".edu" website)

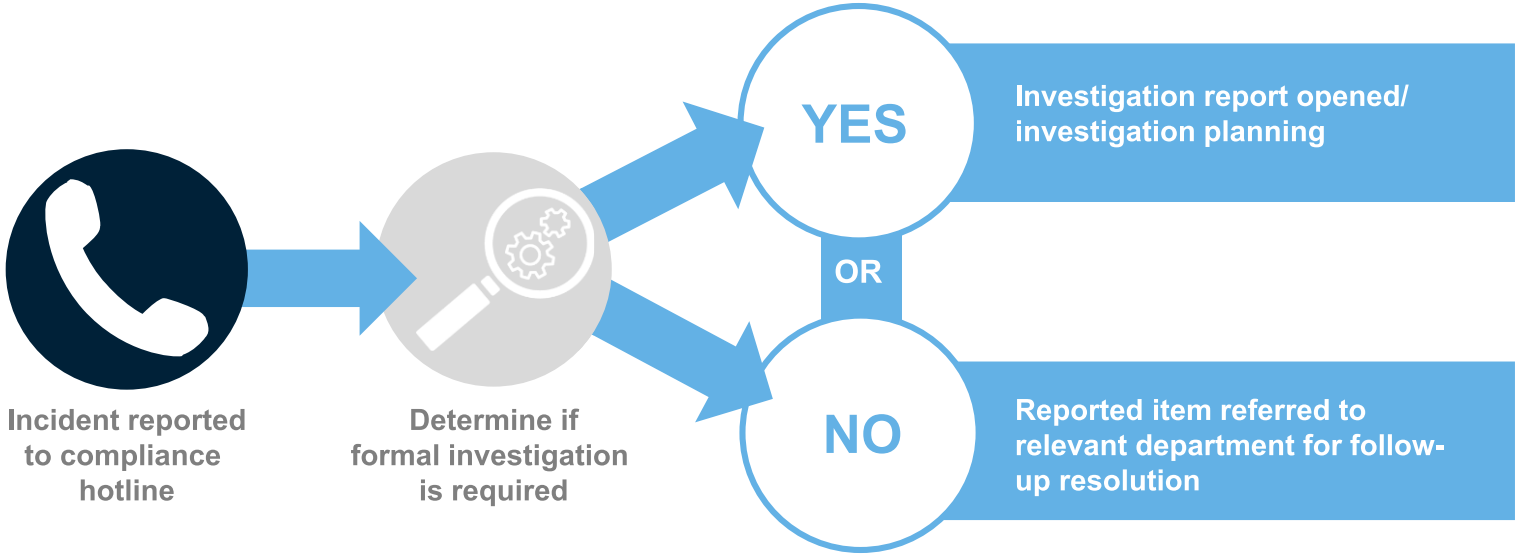
GDPR compliance

- General Data Protection Regulation (GDPR) – new standards for organizations that collect data from European Union (EU) countries
- Emerging area of institutional risk
- IA and Compliance potential audit activities include:
  - IA can perform readiness assessment to identify institutional information/data subject to GDPR; assess current information security processes and procedures
  - Compliance can work with IA to develop standard operating procedures (SOP) for data requests; monitor continued adherence to SOP and communicate SOP to institutional community



Investigations

Compliance is often responsible for ensuring that reported breaches of external laws/regulations, or significant violations of internal policy, are properly investigated



Example investigation process

- Compliance receives a reported allegation (e.g., misuse of P-card by employee) through the hotline or other available anonymous reporting resource
- IA and Compliance collaborate to determine scope and details of the necessary investigation
- IA selects and tests a sample population to assess the compliance of institutional practices and activities and identify areas for improvement or risk to communicate to Compliance
- Compliance develops and implements a plan to address IA's findings and continues regular monitoring activities

Compliance governance assessments

- Potential solution for institutions without a well-defined Compliance program or office
- IA works with institutional leadership to gain a full understanding of current and emerging compliance risks facing the institution (i.e., its compliance risk landscape)
- IA identifies and assesses elements of compliance governance including risk ownership, monitoring and mitigation activities and reporting practices

BAKER TILLY

Case study: compliance assessment

- IA reviewed and assessed risk monitoring and mitigation practices
- Institution did not have a robust centralized Compliance
- IA's audit focused on whether institutional practices were:
  - Appropriately designed to mitigate risk
  - Documented accurately
  - Operating as intended

Case study: compliance risk inventory

- IA assisted management to compile a compliance risk inventory
- IA coordinated with Senior Leadership to:
  - Establish a compliance committee
  - Identify risk owners for each compliance risk area
  - Recommend risk owners for “orphan risks”
- Performed an in-depth assessment of the existence and adequacy of policies and procedures over key compliance areas

BAKER TILLY

Candor. Insight. Results.

Coordinating while communicating

Collaboration when reporting to the Board

Coordinating while communicating

Key functions of the Board of Trustees:

- Review and guide institutional strategy and risk policy
- Monitor effectiveness of institutional governance
- Manage and monitor potential conflicts of interest
- Ensure integrity of accounting and financial reporting systems (e.g., systems for risk management, compliance with the law and relevant standards)
- Oversee disclosure and communications

Board's role in risk governance

George Mason University Board of Visitors

- IA sits on the Audit Committee of the Board
- IA regularly reports audit activity updates throughout the academic year
- Compliance reports to the Board on an annual basis
- Compliance presents updates on the institution's compliance program and the office's efforts to maintain compliance with laws and regulations

BAKER TILLY

Candor. Insight. Results.

Food for thought

Final question for our institutional speakers

BAKER TILLY

Candor. Insight. Results.

>>> In the context of collaboration, how do you respond to the common argument that IA cannot do compliance? <<<

Additional resources

- ACUA connect
- The Society of Corporate Compliance and Ethics (SCCE): http://www.corporatecompliance.org/
- The Institute of Internal Auditors: https://na.theiia.org
- Regulatory compliance: http://www.bakertilly.com/services/risk-internal-audit-cybersecurity/regulatory-compliance/