



## Rethinking Organizational Relationships to Strategically Align Compliance, Audit, Risk, Ethics and ERM Functions



---

---

---

---

---

---

---

---

### Presenters



**Vicki Duggan**  
Chief Compliance, Risk,  
and Ethics Officer  
Montgomery College



**Cassandra Walsh**  
Partner  
Baker Tilly



2

---

---

---

---

---

---

---

---

### Objectives



- > Discuss how institutions identify and leverage opportunities to combine valuable resources and organizational relationships within their institutions
- > Provide ideas for utilizing limited resources to better position your institution while maintaining necessary lines of separation
- > Learn about effective and interesting ways to communicate compliance to educate and build awareness across your institution



3

---

---

---

---

---

---

---

---

**Current Challenges in Higher Education**

BAKER TILLY  
Candor. Insight. Results.

**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

MC

4

---

---

---

---

---

---

---

---

**Identify Institutional Relationships**

BAKER TILLY  
Candor. Insight. Results.

MC

5

---

---

---

---

---

---

---

---

**Define Institutional Relationships**

BAKER TILLY  
Candor. Insight. Results.

**Defining institutional roles and responsibilities**

- > Compliance & Ethics
- > Internal Audit
- > External Audit
- > ERM
- > General Counsel
- > Other Partners

MC

6

---

---

---

---

---

---

---

---

**Define Institutional Relationships**

  
Candor. Insight. Results.

**Establishing distinctions between each strategic relationship**

- > Risk ownership
- > Independence
- > Objectivity
- > Separations



**MC**

7

---

---

---

---

---

---

---

---

**Define Compliance**

  
Candor. Insight. Results.

**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

**MC**

8

---

---

---

---


---

---

---

---

**Define Enterprise Risk Management**

  
Candor. Insight. Results.

- 1 Formalize informal processes that already exist
- 2 Establish a risk management steering committee – President, Vice President for Finance and Administration, Executive Vice President and Provost, General Counsel
- 3 Identify owners of risk (who can set risk tolerance) – President, Vice President for Finance and Administration, Executive Vice President and Provost
- 4 Selected qualitative (as opposed to quantitative) approach to risk assessment
- 5 Identify managers of areas of operating/financial risk (who propose mitigation strategies, manage day-to-day) – academics, athletics, students, HR, facilities, IT, non main campus entities, international activities
- 6 Decided to use heat maps to present results of risk assessments
- 7 Determine integration between ERM process and linkage of risks to the Audit Committee

**MC**

9

---

---

---

---

---

---

---

---

**Define Enterprise Risk Management**

**BAKER TILLY**  
Candor. Insight. Results.

Design ERM Program

Roles and Responsibilities

- > Board of Supervisors
- > Board Oversight Committee – Audit Committee Strategic Risk Owners
- > Vice Presidents

Areas of Risk Assessment

- > Strategic
- > Operating
- > Financial
- > Compliance

**MC** 10

---

---

---

---

---


---

---

---


**The Role of Internal Audit and Compliance**

**BAKER TILLY**  
Candor. Insight. Results.



**Internal Audit**

Internal audit	Cross-functional collaboration results in:	Compliance
<ul style="list-style-type: none"> <li>Concerned with all risks to an institution</li> <li>Operates independently of management</li> <li>Third line of defense</li> </ul>	<ul style="list-style-type: none"> <li>✓ Streamlined processes</li> <li>✓ More efficient use of institutional resources</li> <li>✓ Simplified, direct lines of communication</li> <li>✓ More informed decision making</li> <li>✓ Sound governance and risk management</li> </ul>	<ul style="list-style-type: none"> <li>Concerned primarily with regulatory risk; more restricted scope than IA</li> <li>Ensures compliance with external laws/regulations and policies</li> <li>Second line of defense</li> </ul>



**Compliance**

**MC** 11

---

---

---

---

---

---

---

---

**Aligning Internal Audit and Compliance**

**BAKER TILLY**  
Candor. Insight. Results.

**Developing a common risk language**

<p><b>Improves communication</b> between risk manager(s) and Senior Leadership/ the Board</p>	<p>Allows for a more <b>unified and integrated approach</b> to managing institutional risk</p>	<p>Assists the Board in <b>understanding the integral value</b> of IA and Compliance to the institution</p>

**MC** 12

---

---

---

---


---

---




---


---

**Three Lines of Defense**

  
Candor. Insight. Results.

**Risk management – the role of IA and compliance**

First line	Second line	Third line
 <b>Risk owners or managers</b>	 <b>Risk control and compliance</b>	 <b>Risk Assurance</b>
<ul style="list-style-type: none"> <li>&gt; Operating management</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Limited independence</li> <li>&gt; Reports to management</li> </ul>	<ul style="list-style-type: none"> <li>&gt; IA</li> <li>&gt; Greater independence</li> <li>&gt; Reports to governing body</li> </ul>

 13

---

---

---

---

---

---


---

---

---


---


**Utilizing Limited Resources**

  
Candor. Insight. Results.

**Better positioning your institution for opportunities and efficiencies**

- >How to maintain the necessary lines of separation
- >How to leverage information and resources from peers and professional associations
- >Examples



 14

---

---

---

---

---

---

---

---

---

---

**Leveraging Institutional Relationships**

  
Candor. Insight. Results.

**Opportunities to leverage the expertise of key relationships**

- >How to identify opportunities to partner with others across the institution
- >Combining functions to improve risk management and oversight
- >Examples



 15

---

---

---

---

---

---

---

---

---

---

**Leveraging Institutional Relationships**

BAKER TILLY  
Candor. Insight. Results.

**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**  
 Respond to reported breaches of external laws or violations of internal policies
- Compliance governance assessments**  
 IA assesses and advises Compliance to achieve sound governance

MC

16

---

---

---

---

---

---

---

---

**Collaborative Risk Assessments**

BAKER TILLY  
Candor. Insight. Results.

**Collaborative 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

MC

17

---

---

---

---

---

---

---

---

**Case Study - Collaboration**

BAKER TILLY  
Candor. Insight. Results.

**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:
  - o Identified emerging risks that could affect the institution
  - o Examined current institutional practices for mitigating risk
  - o 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

MC

18

---

---

---

---

---

---

---

---

**Collaborative Audit Activities**

  
Candor. Insight. Results.

**Collaborative 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



**MC**

19

---

---

---

---


---

---

---

---

**Case Study - Collaboration**

  
Candor. Insight. Results.

**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:
  - o Review of policies and procedures; evaluation of internal policy compliance
  - o Identification and testing of key controls
  - o Walk-throughs of facilities and interviews of key process owners

**MC**

20

---

---

---

---


---

---

---

---

**Case Study - Collaboration**

  
Candor. Insight. Results.

**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)

**MC**

21

---

---

---

---

---

---

---

---

**Collaborative Investigations**

**BAKER TILLY**  
Candor. Insight. Results.

**Investigations**

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

```

    graph LR
      A[Incident reported to compliance hotline] --> B[Determine if formal investigation is required]
      B --> C{YES}
      B --> D{NO}
      C --> E[Investigation report opened/investigation planning]
      D --> F[Reported item referred to relevant department for follow-up resolution]
  
```

**MC** 22

---

---

---

---

---

---

---

---

**Collaborative Investigations**

**BAKER TILLY**  
Candor. Insight. Results.

**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
- > Management develops and implements a plan to address IA's findings and continues regular monitoring activities

**MC** 23

---

---

---

---

---

---

---

---

**Collaborative Compliance Assessments**

**BAKER TILLY**  
Candor. Insight. Results.

**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

**MC** 24

---

---

---

---

---


---

---

---




**Case Study - Collaboration**

  
Candor. Insight. Results.

**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:
  - o Appropriately designed to mitigate risk
  - o Documented accurately
  - o Operating as intended

 25

---

---

---

---


---

---

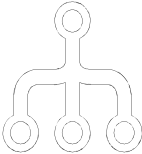
---


---

**Variations in Reporting Relationships**

  
Candor. Insight. Results.

**Variations in reporting relationships**  
*Common organizational structures in higher education*



 26

---

---

---

---


---

---

---

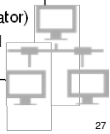
---


**Variations in Reporting Relationships**

  
Candor. Insight. Results.

**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



 27

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

**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

BAKER TILLY  
Candor. Insight. Results.

MC

28

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

**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

BAKER TILLY  
Candor. Insight. Results.

MC

29

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

**Montgomery College – Office of Compliance, Risk and Ethics (Separate Internal Departments)**

*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  
Candor. Insight. Results.

MC

30

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

BAKER TILLY  
Candor. Insight. Results.

**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

MC

31

---

---

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

BAKER TILLY  
Candor. Insight. Results.

**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

MC

32

---

---

---

---

---

---

---

---

---

---

**Variations in Reporting Relationships**

BAKER TILLY  
Candor. Insight. Results.

**Other common IA or Compliance organizational reporting structures**

- > IA and Compliance reporting structure
  - o Chief Financial Officer
  - o Provost
  - o Chancellor
  - o Board of Trustees
  - o Other Senior Leadership

MC

33

---

---

---

---

---

---

---

---

---

---

Q&A



34

---

---

---

---

---

---

---

---