Using a Compliance Program Assessment to Elevate Institutional Compliance Effectiveness

Kevin Robinson
Associate Vice President, Office of Audit, Compliance & Privacy
Auburn University

Michael Somich
Executive Director, Office of Audit, Risk & Compliance
Duke University

Raina Rose Tagle
Partner and National Higher Education Consulting Practice Leader
Baker Tilly

Objectives

I. Discuss proven approaches for assessing your institutional compliance program (even when your program is not formalized) and developing a roadmap for enhancement

II. Apply a Three Lines of Defense framework to evolve management’s ownership of compliance monitoring

III. Assess the maturity of your institutional compliance practices relative to Federal compliance program requirements to gain support for formalizing a compliance program
Agenda

1) Compliance Program Assessment Background
   » Federal Sentencing Guidelines
   » Three Lines of Defense
2) Practical Approaches for Evolving Programs
3) Further Discussion and Questions

Compliance Program Assessment Background:

The Federal Sentencing Guidelines and Three Lines of Defenses
Approaches for Consideration

Perform a self-assessment
Identify and determine how the institution’s compliance risks should be managed

Conduct a compliance program evaluation against the FSG
Serve as a catalyst for the institution’s governance function to develop a compliance program

Utilize peer reviews
Obtain an objective assessment and gain insight into leading industry practices

Federal Sentencing Guidelines (FSG)

What it is:
• Guidelines created by the Sentencing Reform Act of 1984, created by the United States Sentencing Commission.

Who’s included:
• Individuals and organizations convicted of felonies and serious (Class A) misdemeanors.

Purpose of regulation:
• Detail a uniform sentencing policy in the U.S. court system. Courts and prosecutors are required to make choices regarding prosecution, settlement, and the size of fines based on the Sentencing Guidelines.

In addition, the Guidelines detail the requirements of an effective compliance and ethics program for an organization (Chapter 8, Part B2.1 – Effective as of Nov. 1, 2004).
Federal Sentencing Guidelines

7 elements of an effective compliance program

1. Develop appropriate responses to offenses
2. Establish standards and procedures to prevent and detect criminal conduct
3. Assign high-level personnel to oversee compliance
4. Enforce standards through appropriate mechanisms
5. Establish monitoring, auditing, and reporting systems
6. Communicate standards and procedures through training
7. Avoid delegating authority to any individual who has engaged in illegal activities

Program Maturity Assessment

Maturity Levels

1. Initial
   - Unpredictable
   - Limited controls
   - Reactive

2. Repeatable
   - Project focused processes
   - Controls are people-reliable
   - Reactive

3. Defined
   - Organization-wide processes
   - Controls are designed and functioning
   - Proactive

4. Managed
   - Measurable processes
   - Controls are proactively evaluated and tested

5. Optimized
   - Proactively identifies process improvements
   - Automated, measurable controls

The Capability Maturity Model describes a continuum of five stages based on how well a company or organization follows common and repeatable processes to get work done. The low end of the scale describes companies without repeatable processes, where much of the work is chaotic and ad-hoc. The highest end describes companies that use defined and repeatable processes, collect metrics to help them continuously improve their processes, and look for creative ways to do things better on an ongoing basis.

http://www.tenstepm.com/open/A5.1CMMI.html
Three Lines of Defense

According to COFAR:
Institute of Internal Auditors’ Three Lines of Defense in Effective Risk Management and Control

Practical Approaches for Evolving Programs
Introductions

Auburn University
Auburn University – Overview

The opportunity

The players

Building the case

• Facilitating an assessment
• Evaluating existing practices relative to FSG elements
• Addressing the "decentralization challenge"

Considering compliance infrastructure components

The Opportunity and the Players
Approach

Opportunity

• Identify compliance infrastructure options that will best serve to identify Auburn’s compliance requirements, assign accountability, and establish a formal compliance program

Assessment Scope

• Assess the current state of compliance activities at Auburn relative to strong practices in higher education and the FSG
• Explore potential structures and enhanced activities to evolve an institution-wide compliance program

Building the Case

First Steps

Determine a baseline from which progress toward a fully functional compliance program can be measured

Review existing policies, practices, procedures, and internal controls related to the prevention of fraud and abuse

Interview individuals with specific compliance responsibilities and leadership roles

Collaborate with subject matter experts to assess the current state of compliance activities and explore potential structures to evolve an institution-wide compliance program
Compliance Process Maturity Model

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Gaining</td>
<td>The processes that ensure the goals are continuously assessed and adjusted through both incremental and revolutionary improvements. The reputation is maintained in a continuously improving culture.</td>
</tr>
<tr>
<td>Level 2: Managing</td>
<td>Management uses risk management and planning processes to align strategic objectives. The organization uses foresight and priority, while also adapting the processes. The measurable results of a set of actions are documented.</td>
</tr>
<tr>
<td>Level 3: Structured</td>
<td>The results of all aspects of the organization and all stakeholders are communicated.</td>
</tr>
<tr>
<td>Level 4: Formalized</td>
<td>The processes are formally defined and documented. They are performed and monitored according to these documented plans. Where appropriate.</td>
</tr>
<tr>
<td>Level 5: Integral</td>
<td>Processes in the organization are naturally aligned, every activity is aligned, and every role is aligned with the organization's goals. The organization is self-accountable.</td>
</tr>
</tbody>
</table>

Discussion Relative to FSG and Elements

- Standards and Procedures
  - Online policy database
  - Policy review process
  - Prevention and detection
  - Compliance with policies
  - Trainings

- Oversight
  - Board and management oversight
  - Coordinating compliance efforts
  - Compliance inventory
  - Compliance monitoring

- Due Diligence over Delegation of Authority
  - Commitment to the University’s best interests
  - Background checks
  - Technical skills, knowledge, and support

- Communication and Education
  - Comprehensive education and awareness
  - Established training programs
Discussion Relative to FSG and Elements

Monitoring and Auditing
- Monitoring, tracking, and auditing program
- Compliance dashboards or updates
- EthicsPoint

Enforcement and Discipline
- Documented consequences
- Framework, controls, and culture
- Individual accountability and escalation
- Senior leadership involvement

Response and Prevention
- Response and remediation process
- Proactive identification of risks
- Prevention process

Clarify Roles

Contrast Compliance Function Role and Compliance Operational Roles Relative to:

- Standards and Procedures
- Oversight
- Due Diligence over Delegation of Authority
- Communication and Education
- Monitoring and Auditing
- Enforcement and Discipline
- Response and Prevention
Clarify Roles – Oversight Example

### Compliance Function Role

Own the establishment of a University-wide compliance program that adheres to both regulatory requirements and Auburn’s standards as documented in the University’s compliance program. Ensure appropriate/necessary level of involvement and awareness for the program at all levels of management. Perform ongoing evaluation and monitoring of completion of required compliance activities through the monitoring and audit program.

### Compliance Operational Role

Accountable for the actual completion of compliance activities, including assigning process owners among the University’s colleges and departments who are responsible for establishing and implementing the specific compliance activities or serve as liaisons for the effective completion of compliance requirements.

---

## Compliance Infrastructure Considerations

| Benefits | Benefits | Benefits |
| Challenges | Challenges | Challenges |

<table>
<thead>
<tr>
<th>Within IA</th>
<th>Within RMS</th>
<th>Stand-alone Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits</td>
<td>Benefits</td>
<td>Benefits</td>
</tr>
<tr>
<td>Challenges</td>
<td>Challenges</td>
<td>Challenges</td>
</tr>
</tbody>
</table>
Moving Ahead

Current State and Future Outlook

- Designing and establishing a compliance framework
- Identifying and assigning resources
- Outlining and vetting next steps
- Gaining an understanding of best practices and implementation processes

Auburn University
SCCE Higher Education Compliance Conference  
June 5-8, 2016

Duke University

Before:  
July 2004

Decentralized

No clear direction or responsibility

No risk assessment and monitoring plan

Kick-off:  
June 2005

Senior Leadership approved formation of the Compliance Coordinating Committee to identify gaps and create a formal institutional compliance program; the Committee:

Developed a matrix of FSG and the structure of the program to meet FSG requirements

Developed an inventory of laws and regulations by which Duke is required to comply, and identified owners and compliance liaisons for each law/regulation

Duke University – Developed Programs

Establishing program maturity

<table>
<thead>
<tr>
<th>COMPLIANCE PROGRAM STANDARD</th>
<th>GOVERNANCE</th>
<th>PROGRAM DEVELOPMENT &amp; OVERSIGHT</th>
<th>RISK OWNERSHIP</th>
<th>AUDIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of standards and procedures to prevent and detect criminal conduct</td>
<td>Review &amp; approve major compliance policies.</td>
<td>Review and approve major compliance policies.</td>
<td>Provide policy and procedural guidance to liaisons. Provide recommendations to RCSC and AC related to major policies.</td>
<td>Manage operations in accordance with approved policies and procedures. Implement operational controls to support compliance.</td>
</tr>
<tr>
<td>Review reports of compliance activities to evaluate adequacy of standards and procedures.</td>
<td>Review reports of compliance activities to evaluate adequacy of standards and procedures.</td>
<td>Provide guidance to liaisons on key elements to be included in risk assessments, development of monitoring plans and respond to non-compliant behavior. Provide guidance on controls and processes to address identified risks when appropriate.</td>
<td>Ensure appropriate processes are in place to manage compliance risks.</td>
<td>Demonstrate that mechanisms are in place to identify problem areas and to prevent, detect and correct non-compliant behavior. Assist management in ensuring appropriate processes are in place to address compliance risks.</td>
</tr>
</tbody>
</table>
Compliance Liaisons

Defined roles of compliance liaisons – those people managing a compliance operating role

Closely aligned with Auburn

Duke 2007

Institutional Ethics and Compliance Program (IECP)

- Reporting to Duke University Audit Committee
- Administratively report to Executive Director of Internal Audit
- Oversees liaisons
- Manages reporting to senior leaders and board

Compliance Office – School of Medicine (CO-SOM)

- Reports to the Duke University Audit Committee
- Administratively reports to the Chancellor of DUHS
- Audits grants in SOM
- Integrated with Institutional Program
Duke 2014

Consolidate IECP and CO-SOM

- Reports to the Duke University Audit Committee
- Administratively reports to the Chancellor of DUHS

Duke 2015

Decision to move Compliance with Internal Audit

- Formalizing what senior leaders believed
- Next step in maturing compliance
- One reporting line to Audit Committee
- All compliance audit under Internal Audit
Duke University

1st Line of Defense

**MANAGEMENT**
- Culture
- Process (controls, risk tolerance, monitoring)

2nd Line of Defense

**COMPLIANCE**
- Ethics
- Liaison Oversight
- Privacy Program
- Advisory/Facilitation Coordination
- Centralized Review Programs
  - HIPAA
  - Human Subject Research Compliance
  - Department - Highest Priority Risks

3rd Line of Defense

**AUDIT**
- Horizontal Process
- Vertical Departments with Identified or Suspected Challenges
- Investigations Coordination

Discussion
Lessons Learned

Any questions?
Contact Information

Kevin Robinson, CIA, CFE, CCEP  
Associate Vice President, Office of Audit, Compliance & Privacy, Auburn University  
robinsonmk@auburn.edu  
334-844-4389

Michael Somich, CPA  
Executive Director, Office of Audit, Risk and Compliance, Duke University  
mike.somich@duke.edu  
919-613-7611

Raina Rose Tagle, CPA, CIA, CISA  
Partner, National Higher Education and Research Institutions Consulting Practice Leader, Baker Tilly  
raina.rosetagle@bakertilly.com  
703-923-8251

http://www.bakertilly.com/industries/higher-education/

Required disclosures

> This 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.

> Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International.
Appendix

Conducting a Compliance Program Audit

Approaches for Conducting a Compliance Program Audit

> Use the FSGO’s seven elements to provide a systematic and structured approach.
> Determine that programs and procedures exist and are well designed to support the seven FSGO elements.
> Assess the effectiveness of each of the seven elements.
Conducting a Compliance Program Audit – Standards and Procedure

Standards and Procedures

Review and analyze key compliance policies and procedures, along with the approval process for implementing new procedures.

➢ Is there a process for implementing new and updating old policies (e.g., a checklist that outlines the required action steps necessary for obtaining final approval)?
➢ For certain policies (e.g., “Employee Code of Conduct”) does the organization require that employees acknowledge that they have read and understood the policy?

Conducting a Compliance Program Audit – Ownership

Ownership

Review the current compliance infrastructure or organizational structure.

➢ Who owns the compliance process in the organization?
➢ Is there a compliance officer or figurehead?
➢ To whom do they report?
Avoiding Delegation to Questionable Individuals

Assess the effectiveness of the background check process to avoid the delegation of authority to individuals who have engaged in illegal activities.

- What background check procedures presently exist?
- Do written policies and procedures exist? If written policies do not exist, interview knowledgeable people as to the informal background check procedures that have traditionally been followed.
- Are the people performing the background checks qualified to do so?
- Is adequate documentation maintained on all background checks?
- Are the backgrounds of all new hires checked with no exceptions?
- What, specifically, is checked: degrees conferred, certifications, credit history, criminal record, previous employment, references?

Communication

Review current training and outreach programs that provide employees with knowledge about compliance requirements and issues in the organization.

- Does the organization provide formal training (e.g., new hire orientation)?
- Does it provide informal training (e.g., staff luncheons)?
- Does the organization provide web-based trainings?

Review existing compliance materials and resources, including a compliance website.

- Does the organization maintain a compliance webpage?
- Does it provide a list of positions, by subject area, responsible for overseeing compliance in the organization?
- Does each position have a webpage that provides a listing of the laws and regulations associated with each position, and does it provide links to resources and related organization policies?
Conducting a Compliance Program
Audit – Monitoring

Monitoring
Evaluate the current monitoring and reporting processes.
> Is the monitoring process centralized or decentralized?
> Are regular risk assessments performed?
> Who is responsible for performing risk assessments?
> Are personnel who have key compliance roles interviewed?
> How are issues reported, documented, and resolved?

Conducting a Compliance Program
Audit – Enforcement

Enforcement
Review current enforcement and discipline processes.
> Are there appropriate mechanisms in place for individuals who fail to detect an offense?
> What are potential corrective actions for failure?
Conducting a Compliance Program Audit – Response

Response
Review and evaluate current mechanisms in place for responding and preventing future offenses.

- What steps are taken to respond to offenses?
- Are these steps reasonable?
- What steps are taken to prevent further similar offenses?
- Is a modification of the response process needed to prevent further offenses?

Conducting a Compliance Program Audit – What if there is no Compliance Program?

If there is no compliance program in place, begin by...

- Understanding the government's view of risk
  - Agency audit work plans
  - Recent investigations
  - Government interpretations of statutes
- Conducting a self-assessment
  - Determine a baseline from which progress toward a fully functional compliance program can be measured.
  - Review existing policies, practices, procedures, and internal controls related to the prevention of fraud and abuse
  - Serving as a catalyst for the organization's governance function to evolve a program