Developing, Implementing and Auditing an Effective University-Wide Compliance Office

Eric Groen, Managing Director
Beth Boyle, Associate Director

September 14, 2016

Introduction

Eric Groen – Managing Director
Eric Groen is a Managing Director with Protiviti, based in the Phoenix area. He has over 15 years of experience in consulting and audit, including both internal and external audit experience. Eric’s experience extends across a number of industries, however, he spends the majority of his time focusing on higher education and more specifically compliance and governance issues.

Eric has a B.S. degree in Accounting and Finance from Creighton University, is a Certified Public Accountant, a Certified Internal Auditor, and a Certified Compliance and Ethics Professional.

Beth Boyle – Associate Director
Beth is an Associate Director in the DC and NY regions. Beth has over 17 years of experience in internal and external audit, business consulting and related services. She delivers Internal Audit and SOX services to a variety of clients, primarily in the higher education, government contracting and professional services industries.

Beth is a Certified Public Accountant (CPA) and a Certified Internal Auditor (CIA) and holds a B.S. degree in Accounting from Boston College and a M.B.A from St. Mary's College of California.
Today’s Areas of Focus

1. Identify key benefits of a proactive compliance program.

2. Achieve these key benefits by learning the key attributes, practices and components of an effective Compliance Program.

3. Use the key attributes, practices, and components to develop an audit plan to evaluate the compliance program at your University.
You are Not the First, and You are Not Alone

According to a 2013 Bi-Partisan Senate Task Force, in their document entitled “Recalibrating Regulation at College and Universities”, they quote the American Action Forum calculation that Institutions spend 26.1 million hours annually completing Dept. of Education mandated forms.
### Key Benefits

<table>
<thead>
<tr>
<th>Frameworks</th>
<th>Frameworks can bring consistency and oversight of key compliance issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility and Reporting Lines</td>
<td>A chief compliance officer and institution-wide compliance committee can provide leadership and enhance decision making processes.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>A robust risk assessment process can identify and prioritize risks.</td>
</tr>
<tr>
<td>Compliance Training</td>
<td>Comprehensive compliance training programs are one of the key factors in the success of a Compliance Program.</td>
</tr>
<tr>
<td>Compliance Monitoring</td>
<td>Monitoring to detect non-compliance and self-reporting can limit prosecution, fines, and reputational damage.</td>
</tr>
</tbody>
</table>

“The government has made it clear that companies who take compliance seriously and are committed to finding, fixing, and solving legal and regulatory problems are in a far better position than those who do not invest in real, robust, and effective compliance programs. I can think of no better proof of the value of strong compliance and ethics programs than the DOJ’s and SEC’s recent actions.” SCCE Chief Executive Officer Roy Snell

### Compliance Program

**IIA Position Paper:**

*The Three Lines of Defense in Effective Risk Management and Control (January 2013)*

#### The Three Lines of Defense Model

1. **1st Line of Defense**
   - Management Controls
   - Internal Controls Measures

2. **2nd Line of Defense**
   - Financial Controls
   - Risk Management
   - Quality
   - Environment
   - Compliance

3. **3rd Line of Defense**
   - Financial Audits

“...the compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management, and in some business sectors, directly to the governing body. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring.” IIA
Key Attributes, Practices and Components of an Effective Compliance Program

Federal Sentencing Guidelines

- Response to Criminal Conduct or Non-Compliance
- Standards, Policies and Procedures
- Incentives and Disciplinary Actions
- Assignment of Responsibilities
- Communication, Awareness and Training
- Due Diligence and Delegation of Authority

Assessments and Continuous Improvement

Monitoring, Auditing and Assessing the Program

Oversight & Accountability

Documentation & Reporting

Ongoing Improvement
Elements of a Compliance Management System (CMS)

- Establishes its compliance responsibilities;
- Communicates those responsibilities to employees;
- Ensures that responsibilities for meeting legal requirements and internal policies are incorporated into business processes;
- Reviews operations to ensure responsibilities are carried out and legal requirements are met;
- Takes corrective action, and
- Updates tools, systems, and materials, as necessary.

Protiviti’s Compliance Framework (PCF)

Protiviti’s Compliance Framework

- Incorporates the key components of effective regulatory compliance programs from a regulatory perspective
- Integrates the principles of effectiveness, efficiency, comparability, communication, and reporting
- Identifies and defines specific risks associated with each stage of the PCF
- Provides a roadmap to evaluate the effectiveness of the compliance programs
Assign Responsibility and Accountability

The Board of Trustees and Senior Management should designate a knowledgeable compliance officer to administer the compliance program. The board and senior management must grant the compliance officer sufficient authority and independence to cross departmental lines, access to all areas of the company, and effect corrective action when needed.

Leading Practices

- Formal Designation by Board of a qualified Compliance Officer
- Reporting Lines for Compliance Officer and Department
- Establishing Compliance Department with Documented Responsibilities
- Establishment of a strategic, enterprise-wide management Compliance Committee
- Periodic Evaluation of Compliance Resources
- Operational responsibilities of Compliance personnel are limited and appropriate segregation of duties exists
Compliance Office - EXAMPLE

Primary Responsibilities:
- Administer Code of Conduct and other organizational policies, including a policy on policies.
- Operate currently existing Anonymous Reporting Line including investigations, as necessary.
- Provide independent/objective compliance monitoring function
- Administer Conflicts of Interest policy.

Leadership – Option 1 – Chief Compliance Officer Model

Reporting Lines:
- Dual reporting to Audit (and Compliance) Committee and the President. Direct reporting line to Audit (and Compliance) Committee, 'dotted line' (indirect or administrative) reporting to the President.
- Personnel with responsibilities around compliance will establish a 'dotted line' (indirect) reporting relationship to the Compliance Leader.
- Compliance Leader could be allocated at least one full-time employee to support compliance at a university level.
- Dotted line (Indirect) reporting relationship with General Counsel to establish and maintain Attorney Client Privilege, as necessary.
- Internal Audit has an oversight role and is responsible for independently validating the operating effectiveness of the compliance organization.
Future Compliance Organization Structure:
Option 2 – Director of Compliance Model

Reporting Lines:
- Dual reporting to Audit (and Compliance) Committee and the Chief Operating Officer. Direct reporting line to the Chief Operating Officer, 'dotted line' (indirect or administrative) reporting to the Audit (and Compliance) Committee, as required.
- Personnel with responsibilities around compliance will establish a 'dotted line' (indirect) reporting relationship to the Compliance Leader.
- Compliance Leader could be allocated at least one full-time employee to support compliance at an enterprise level.
- Dotted line (indirect) reporting relationship with General Counsel to establish and maintain Attorney Client Privilege, as necessary.
- Internal Audit has an oversight role and is responsible for independently validating the operating effectiveness of the compliance organization.

Office of University Integrity

Primary Responsibilities:
- Administer University Code of Conduct to be created
- Operate currently existing Anonymous Reporting Line and independent “Tier 2” monitoring function
- Oversee the revised University Policy Process
### Inventory Business Activities

**Compliance Program Element**

Compliance and Legal personnel should be informed as to the company’s business activities including new program development and change management processes.

<table>
<thead>
<tr>
<th>Leading Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attendance of Compliance personnel in various institution-wide committees</td>
</tr>
<tr>
<td>Active Participation of Compliance Personnel in Change Management Process</td>
</tr>
<tr>
<td>Establishing Policies and Procedures related to New Programs</td>
</tr>
<tr>
<td>New Business Activities to involve review and feedback from Compliance Personnel</td>
</tr>
</tbody>
</table>

### Inventory Legal and Regulatory Requirements

**Compliance Program Element**

Compliance personnel should identify and document the applicability of legal and regulatory requirements to both new and existing business operations.

<table>
<thead>
<tr>
<th>Leading Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating and Maintaining Inventory of applicable legal and regulatory requirements</td>
</tr>
</tbody>
</table>
| Good place to start: Higher Education Compliance Alliance  
http://www.higheredcompliance.org/matrix/ |
| Monitoring through Multiple Sources the new laws and regulations; Online subscription to updates from relevant regulators, various industries publications etc. |
| Communicating regulatory updates |
Assess Risk

The company should periodically assess the risk of non-compliance with regulatory compliance requirements and the risk of criminal conduct occurring.

- Conducting comprehensive enterprise-wide compliance risk assessments periodically
- Driving Compliance Program through Risk Assessment Results
- Identified gaps are tracked and monitored centrally (i.e., issues log) and assigned to appropriate process owners for prompt resolution and accountability

Define Policy

The institution should establish a formal, written compliance program administered by a designated chief compliance officer. The written program should also represent an essential source document that will serve as a training and reference tool for all employees.

- Developing Written Compliance Program and Periodically Reviewing it
- Establishing Formal Policy Framework
- Periodically updating Written Compliance Program for changes to Legal and Regulatory Requirements
- Accessibility of Written Policies to Employees
Establish Procedures

### Compliance Program Element

Compliance procedures should be detailed in written form and updated as the Institution’s environment changes. Appropriate procedures should be developed to accomplish goals and objectives, as set forth by the company’s policies. Policies and procedures should also provide personnel with sufficient information needed to perform a business transaction in a manner designed to prevent violations and to detect or prevent associated risks of harm to consumers.

<table>
<thead>
<tr>
<th>Leading Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration among process owners and Compliance in developing formal, written compliance-related procedures</td>
</tr>
<tr>
<td>Establishing Formal Procedure Framework</td>
</tr>
<tr>
<td>Accessibility of Written Procedures to Employees</td>
</tr>
<tr>
<td>Compliance-related procedures complement and do not contradict established policies and other procedures</td>
</tr>
<tr>
<td>Key process owners and business managers review and approve compliance-related procedures on an annual basis</td>
</tr>
</tbody>
</table>

Provide Training

### Compliance Program Element

All employees including the Board of Trustees should receive relevant training that covers applicable regulations, laws, and internal policies / procedures.

<table>
<thead>
<tr>
<th>Leading Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Needs Periodically Reviewed</td>
</tr>
<tr>
<td>Developing Compliance Training in accordance with Risk Assessment Results</td>
</tr>
<tr>
<td>Customizing Training Content</td>
</tr>
<tr>
<td>Tracking Employee Comprehension and completion</td>
</tr>
<tr>
<td>Completion of Compliance Training by the existing and new employees</td>
</tr>
<tr>
<td>Periodic compliance training is provided to the Board</td>
</tr>
</tbody>
</table>
## Monitor Compliance

**Compliance Program Element**

The institution must take reasonable steps to ensure that compliance and ethics programs are followed, including monitoring to detect non-compliance, and periodically evaluating the effectiveness of such programs.

#### Leading Practices

- Establishing Comprehensive Compliance Monitoring and Testing Schedule
- Implementing Formal, Written Compliance Monitoring and Review Procedures
- Reviews and Testing Conducted Accurately
- Furnishing of Monitoring and Testing Results
- Tracking Issues and Management Responses

## Resolve Consumer Complaints and Monitor Trends

**Compliance Program Element**

An effective compliance management system should ensure that a company is responsive and prompt in handling complaints and inquiries from all constituencies, including employees, faculty and students. Procedures should be established for addressing complaints, and individuals or departments responsible for handling them should be designated and known to all company personnel to expedite referrals.

#### Leading Practices

- Defining Complaint Resolution Policies and Procedures
- Regulatory Complaints Processed or reviewed by the Compliance or Legal function
- Central Repository developed to Track and Categorize Complaints Received
- Analyzing Complaint Trends
- Complaint Resolution Activities Reporting to Senior Management / Board
## Remediate Identified Compliance Deficiencies

### Compliance Program Element

Management should establish processes to manage internal and external regulatory reviews, audits and examinations. Management should coordinate these activities and track compliance-related findings and ensure appropriate, sufficient, timely and complete corrective action.

### Leading Practices

- Formally Assigning Responsibilities for managing compliance-related internal audits and regulatory examinations
- Tracking Compliance-Related Audit deficiencies
- Notification of Findings and Deficiencies to Senior Management
- Furnishing status of Outstanding Compliance Issues
- Tracking Issues and Management Responses

---

## Manage Regulatory Examinations

### Compliance Program Element

Institutions should establish a formal process to manage regulatory examinations and other requests from / interaction with their supervisory agencies such as the Department of Education or accreditors.

### Leading Practices

- Identifying Central Point of Contract for regulatory examiners
- Tracking Central Point of Contract and Assigning Due Date for Each Item of Information, Exam “First-Day” Letter
- Process to Validate Accuracy and Completion of Information provided to examiners
- Ability to reproduce all Information Provided to Examiner
- Controls to ensure Examiners are Directed to Appropriate Process Owners
- Tracking of Commitments made to Regulators
### Report To Leadership

**Compliance Program Element**

Executive management and the Board of Trustees should receive regular reports concerning the effectiveness of the company's compliance program.

#### Leading Practices

- **Furnishing Compliance to Senior Management periodically and Management and Board Committee Reporting Includes:**
  - Results of the periodic compliance risk assessment
  - Updates regarding changes to regulatory requirements and the regulatory environment
  - Key compliance risks associated with new business initiatives and how those are being addressed
  - Compliance monitoring / testing results
  - Status of compliance training
  - Status of compliance-related issues
  - Complaints activities

---

### Leading Compliance Practices

The following considerations provide a blueprint for establishing and maintaining an effective enterprise-wide compliance program:

- **Set Tone at the top**
- **Establish a structure that works**
- **Form Compliance Committee**
- **Periodic Compliance Risk Assessment**
- **Proactive monitoring and testing of compliance risk**
- **Compliance training program**
- **Develop comprehensive training tools**
Audit Effectiveness of Compliance Program

The institution should periodically conduct independent audits of the effectiveness of its compliance risk management program.

Leading Practices

- Assessing Compliance in the Development of Internal Audit Plan
- Compliance Audits conducted by Qualified Personnel
- Address Completeness and Accuracy of Audits
- Furnishing of Audit Results
- Tracking Issues and Management Responses

Internal Audit’s Role in Compliance


The Three Lines of Defense Model

- Operational efficiency and effectiveness
- Safeguarding of assets
- Reporting reliability and integrity
- Compliance with laws, regulations, policies, procedures, and contracts.
- All elements of the risk management and internal control framework
- All levels and units of operation

Adapted from EU/ETSI Guidance on the 8th EU Company Law Directive, article 41
Develop an Audit Plan to Evaluate the Compliance Program

### Effective Internal Audit – Third Line of Defense

Developing the Internal Audit infrastructure is a critical first step to starting an effective Internal Audit function.

<table>
<thead>
<tr>
<th>Draft Internal Audit Charter</th>
<th>Identify Risk</th>
<th>Assess and Prioritize Risk</th>
<th>Select Focus Areas</th>
<th>Develop and Approve Audit Plan</th>
</tr>
</thead>
</table>
| • Provide template consistent with the International Standards for the Professional Practice of Internal Auditing (IIA Standards)  
• Customize the Internal Audit Charter to meet the needs of the organization. | • Review industry risks  
• Create a customized risk catalog  
• Distribute draft Business Risk Model to executive management for feedback | • Prioritize risk based on Risk Model and executive feedback  
• Create surveys to address key risk areas  
• Meet with and discuss surveys with key management  
• Compile, aggregate, and analyze results | • Evaluate/prioritize focus areas  
• Meet with key executives to discuss preliminary risk assessment results  
• Define preliminary listing of projects to address areas of risk | • Determine overall budget allocation  
• Develop scope statements and level of effort for proposed projects  
• Obtain senior management and Audit Committee approval |
The Third Line’s Two-Pronged Approach

Internal Audit Assessments

Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives.

Leading Practices

- Individual Areas of Compliance / Individual Functions that own and Manage Risks.
- The Overall Compliance and Risk Management Function

Assessment Methodology and Approach

1. **Protiviti Compliance Framework**
   - Define compliance objectives
   - Customize the Compliance Framework

2. **Identify CoRs**
   - Compile comprehensive list of CoRs
   - Interview owners of known compliance objectives

3. **Evaluate CoRs**
   - Determine current state of compliance risk management practices
   - Analyze CoRs using the Capability Maturity Model (CMM)

4. **Develop Action Plans**
   - Perform gap analysis for compliance areas identified
   - Benchmark compliance attributes against other processes, institutions and industries
Categories of Requirements (CoR)

- "High-level" groupings designed to encompass numerous laws and regulations applicable
  - Serve as a base from which to conduct detailed assessment in the future
- May span multiple departments and operations
- Certain CoRs (e.g., Anti-Corruption, Code of Conduct / Ethics, etc.) universal among various industries

<table>
<thead>
<tr>
<th>Infrastructure Element</th>
<th>Key Descriptions of Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Structure and Accountability</td>
<td>Key tasks are assigned to people with the requisite knowledge, skill, and expertise. Roles and responsibilities must be defined and delineated.</td>
</tr>
<tr>
<td>Requirements Identification</td>
<td>In order to be efficient and effective, identified compliance requirements must be aligned with business processes.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>In order for management to make informed decisions a formal risk assessment is required.</td>
</tr>
<tr>
<td>Standards and Controls</td>
<td>Standards and controls provide key company stakeholders with a common understanding and a key set of guidelines.</td>
</tr>
<tr>
<td>Training</td>
<td>Training is essential to the development of people and the compliance function.</td>
</tr>
<tr>
<td>Monitoring and Remediation</td>
<td>Monitoring and remediation should:</td>
</tr>
</tbody>
</table>

Together the Infrastructure Elements and CMM provide a concise view of process effectiveness
Each CoR identified is evaluated against the components of the infrastructure elements and the maturity level of each is assigned a rating:
- Current-state maturity levels are assigned in relation to detailed, pre-defined capability stages for each level
- Results are displayed in a CMM format
- Results are aggregated to:
  - Illustrate the overall maturity levels of each CoR and of each infrastructure element
  - Facilitate benchmarking analyses

**Key Characteristics of Compliance Maturity**

<table>
<thead>
<tr>
<th>Description</th>
<th>Key Characteristics of Compliance Management Maturity</th>
</tr>
</thead>
</table>
| Optimized Continuous Improvement | Compliance is a source of competitive advantage  
  - Centralized compliance functions provide consistent excellence  
  - Compliance is aligned with our overall strategy and culture  
  - Emphasis is placed on continuous improvement |
| Managed Quantitatively Managed | Compliance is quantitative and aggregated enterprise-wide  
  - Rigorous compliance management elements are applied to enterprise-wide risks  
  - Fact-based debates occur on the risk/reward trade-off for implementing further compliance activities  
  - Processes are monitored with automated controls and managed by exception  
  - Thorough cross-training and a fully integrated infrastructure that is not dependant on key individuals |
| Defined Qualitatively Managed | Compliance is measured and managed primarily qualitatively  
  - Uniform compliance management elements are defined and institutionalized  
  - Compliance management infrastructure elements are in place; still require improvement  
  - Ownership is defined and accountability is enforced. |
| Repeatable Intuitively Managed | Compliance management processes are established and repeating.  
  - Risk response effectiveness relies on quality people assigned to tasks  
  - Initial compliance management infrastructure elements are developed  
  - Standards are inconsistent and controls are largely manual and detective |
| Initial / Ad Hoc Dependent on Heros | Compliance management efforts are dependent on individuals and “fire fighting”  
  - Limited or incomplete infrastructure to manage compliance  
  - Compliance response effectiveness is ad hoc and incorporates undefined tasks  
  - Reliance on key people and their initiative  
  - “Just Do It” mentality |
Develop Action Plans

- For each CMM developed by CoR and/or infrastructure element, compare the maturity rating to the comparable ratings to other areas in the institution, or to other industry specific criteria, as appropriate.

- The benchmark ratings should contain strengths as well as improvement opportunities that articulate how the institution can strategically address gaps in their programs.

Develop Action Plans – Sample Reporting
Develop Action Plans – Sample Reporting

Optimized
Managed
Defined
Repeatable
Initial

Current State
Future State

Infrastructure Elements
Organisational Structure and Accountability
Requirement Identification
Risk Assessment
Standards and Controls
Training
Monitoring and Remediation

Future State Compliance Attributes

Compliance Programs...

Other Universities have already begun their journey, where are you?
Questions

Contact Information

Eric Groen
Managing Director
Phone: +1 602.273.8341
eric.groen@protiviti.com

Beth Boyle
Associate Director
Phone: +1 571.382.7240
beth.boyle@protiviti.com

Powerful Insights. Proven Delivery.™