Monitoring Mentor: The Workshop

SCCE HIGHER EDUCATION CONFERENCE
6/3/2018

AGENDA

Introduction
Monitoring Framework
Activity
Monitoring Program
Monitoring Controls
Case
Activity
Case
Recap

Your Coach

Jessica Wasserman is an experienced professional with a diverse business and operational background. Over the past 9+ years, she has developed expertise in the areas of governance, risk, and compliance. As Assistant Compliance Officer for New York University (NYU), Jessica leads a variety of initiatives and programs focused on ensuring adherence to different laws, regulations, policies, standards, and best practices governing higher education institutions. Prior to joining NYU’s Office of Compliance and Risk Management, Jessica led efforts to implement and operationalize NYU’s Enterprise Risk Management Program.

Earlier in her career, Jessica enjoyed working for top business organizations like PricewaterhouseCoopers (PwC Advisory), Siemens (Siemens Energy, Inc.), and The Walt Disney Company. Jessica is a certified Six Sigma Green Belt and MBA Candidate at NYU’s Leonard N. Stern School of Business.

285 Mercer Street, 5th Floor
New York, NY 10003
Office: 212-992-8348
Mobile: 646-530-1931
Email: jessica.wasserman@nyu.edu
Essential Elements of an Effective Compliance Program

1. Establish policies, procedures and controls;
2. Exercise effective compliance oversight;
3. Exercise due diligence to avoid delegation of authority to unethical individuals;
4. Communicate and educate employees on the compliance program;
5. Monitor and audit the compliance program for effectiveness;
6. Ensure consistent enforcement and discipline of violations; and
7. Respond appropriately to incidents and take steps to prevent future incidents.

A little bit about “Monitoring”

The concept of monitoring can be found in multiple types of practices. It is used to determine the effectiveness of other activities.

Compliance Program Evolution

The evolution of NYU’s compliance monitoring program is currently ongoing. Below is a look at the progress we made as well as our future.
Before you dive into developing your monitoring framework, consider and ask yourself the following questions:

- What is the vision, mission, and objectives that you/your department/your organization would like to accomplish?
- What is the structure of your compliance program (e.g., centralized, decentralized or hybrid)?
- What do your current monitoring activities look like (e.g., substantive areas, activities)?
- What financial and non-financial (e.g., talent) resources or constraints are you subject to?
- Is there overlap or redundancy in monitoring between functions or departments?
Constraints

Below are some types of constraints that compliance functions may be subject to at higher education institutions.

- Financial Resources
- People/Headcount
- Knowledge/Technology
- Policies and Procedures
- Structure/Culture

- Limited budget
- Limited staff
- Limited expertise
- Limited automation
- Organizational structure and reporting lines

Framework Overview

A framework basic underlying structure or approach that organizes ideas and guides activities.

Create Monitoring Framework

A framework basic underlying structure or approach that organizes ideas and guides activities.

- Assess
- Develop
- Execute
- Review

- Legal and regulatory environment
- Current risk or compliance monitoring practices
- Identify stakeholders and subject matter experts
- Document processes and controls
- Conduct monitoring and testing activities
- Document results
- Communicate and report findings
- Review processes and results
- Make improvements and changes as necessary
Additional Example

Vision: Strong integrated monitoring function.
Mission: To educate stakeholders about compliance requirements and best practices through the monitoring process.
Objectives: Document compliance process and controls. Teach stakeholders how to identify controls and conduct objective monitoring activities.

Constraints:
- Time/Personnel
- Limited influence and accountability
- Limited expertise
- Limited data

Monitoring Program

When building your program...

- Leverage what you know and what you have (e.g., experience and deliverables)
- Be ambitious and be practical (e.g., develop a plan that provides solid guidance and increases product quality)
- Connect it to your Compliance Program and institutional goals
- Define and describe
- Don’t succumb to perfection (e.g., the monitoring plan should be reviewed and refined periodically)
Standard Features

While compliance monitoring programs should be tailored to the institution, we do see some standard elements included in them.

I. Introduction
   A. Background on compliance monitoring initiative.
   B. Goals and objectives.
   C. Governance and authority support.

II. Monitoring Framework and/or Methodology
   A. Define the different types of monitoring activities (e.g., direct, indirect, on demand).
   B. Define general scope (e.g., taking into account objectives and constraints).
   C. Difference between compliance monitoring and internal audit.

III. Testing and Control Activities
   A. Definition and clarification (e.g., types of controls, testing types, etc.)
   B. Testing plan and documentation information
   C. Templates and other tools

IV. Monitoring Calendar

Monitoring Documentation

Below is some guidance around documenting monitoring activities for compliance risks and projects.

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>What is the compliance risk being monitored?</td>
</tr>
<tr>
<td>II</td>
<td>How is the risk being monitored?</td>
</tr>
<tr>
<td>III</td>
<td>Are there any associated system controls?</td>
</tr>
<tr>
<td>IV</td>
<td>Is monitoring applied to individual or to overall compliance risk?</td>
</tr>
</tbody>
</table>

Monitoring Calendar

A Monitoring Calendar is what we call our monitoring project plan for the year. We identify compliance monitoring activities and map them to a specific time period.
Monitoring Controls

What are controls?

Identifying, documenting, and testing controls can be difficult for stakeholders including compliance officers.

There are three types of controls:
- Preventive – Designed to keep errors or irregularities from occurring
- Detective – Designed to detect errors or irregularities that may have occurred
- Corrective – Designed to correct errors or irregularities that have been detected*  

Please note that controls are not perfect and can fail due to various reasons like overrides, human or technology error, etc.  


How do I identify controls?

To identify controls, one needs to understand the process. Documenting a particular process step-by-step is one of the easiest ways to identify controls.  

A good way to visualize a process is to develop a process flow diagram.
Case 1 – Conflicts of Interest

Monitoring Steps Overview:

1. Prepare and send out automated annual conflict of interest disclosures to stakeholders.
2. Once disclosures are received, we review responses with disclosures of potential conflicts.
3. A compliance officer follows up with the employee regarding potential conflicts. This compliance officer checks for previous disclosures and investigates the facts. Interviews are conducted.
4. A conflict mitigation plan is implemented (if needed).

Ad hoc conflict of interest reports are collected year-round. We use an online platform to collect and track our conflict of interest disclosures.

Case 1 – Conflicts of Interest

Identifying, documenting, and testing controls

Key Compliance Controls:
- Governance
- Policy
- Procedures
- Training
- Monitoring

CDI-Specific Controls:
- System or form-related (e.g., research, procurement)
- Conflict Management Plan

Monitoring Controls Activity
Case 2 - HEOA

Monitoring Steps Overview:

1. Review regulatory information and consult with stakeholders to understand if there have been any updates to HEOA regulations or guidance.
2. Update HEOA matrix/chart that details the regulatory requirements.
3. Review website for HEOA requirements that are published or accessible online.
4. Contact stakeholders to obtain insight into update and completion of other requirements.
5. Report any gaps and advise on mitigation activities.

<table>
<thead>
<tr>
<th>Scope Area</th>
<th>Testing Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of institutional information</td>
<td>Confirm notices sent out regarding FERPA and information posted online</td>
</tr>
<tr>
<td>Availability of tuition, financial aid information and resources</td>
<td>Confirm information regarding the cost of attending is available as well as access to the net price calculator</td>
</tr>
<tr>
<td>Policies for transfer credits, refunds in case of withdrawal</td>
<td>Check access to policies online. Confirm they were reviewed and updated.</td>
</tr>
<tr>
<td>Provide NYU information on College Navigator website</td>
<td>Confirm NYU information was reviewed, updated and submitted to the Government’s College Navigator website.</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>Confirm information regarding financial aid is accessible online. Confirm policies on eligibility for financial aid were reviewed and updated.</td>
</tr>
<tr>
<td>Health &amp; Safety</td>
<td>Confirm statistics is published regarding alcohol and drug abuse violations. Confirm policies on tobacco use and relevant laws were reviewed</td>
</tr>
</tbody>
</table>
List of Common Compliance Risk Areas – For Monitoring

<table>
<thead>
<tr>
<th>Area</th>
<th>Risk Area</th>
<th>Risk Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA</td>
<td>Environmental Health &amp; Safety</td>
<td>Tax-exempt Bonds</td>
</tr>
<tr>
<td>Title II</td>
<td>Hazard/Campus Safety</td>
<td>Title IV/ Campus Safety</td>
</tr>
<tr>
<td>Title IV</td>
<td>Conflicts of Interest</td>
<td>Financial Aid</td>
</tr>
<tr>
<td>Prevention on Campus</td>
<td>Supply Controls</td>
<td>Other Research Privacy Requirements</td>
</tr>
<tr>
<td>FERPA</td>
<td>Health Information (e.g., PHI)</td>
<td>Discrimination and Affirmative Action</td>
</tr>
<tr>
<td>FERPA</td>
<td>Interest Grant Management</td>
<td>Federal W2 Reporting</td>
</tr>
<tr>
<td>FERPA</td>
<td>Industry Accreditation</td>
<td></td>
</tr>
<tr>
<td>Red Flags</td>
<td>International Offices</td>
<td>Completed Risk Projects</td>
</tr>
<tr>
<td>Reporting Line</td>
<td>Code of Conduct/Review/Training</td>
<td>State &amp; City Compliance Requirements</td>
</tr>
</tbody>
</table>

HIPAA Monitoring Example

Monitoring Steps Overview

1. Spoke with other functions (e.g., Internal Audit, Compliance and Risk Steering Committee)
2. Identified HIPAA scope; what departments or business units were covered or at risk
3. Researched HIPAA audit protocol (e.g., published by OCR)
4. Selected business unit to monitor
5. Requested documents (e.g., policies, training, governance) for review
6. Conducted limited testing and documented findings
### HIPAA Monitoring Example

#### Identifying the control, scope, and testing activities

<table>
<thead>
<tr>
<th>Type</th>
<th>Action</th>
<th>Scope Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Review applicable policies and procedures.</td>
<td>- Uses of Privacy Protocols - Notice of Privacy Practices - Confidential communications - Accessing of PHI</td>
</tr>
<tr>
<td>Training</td>
<td>Review training and training requirements.</td>
<td>- Training provides overview of HIPAA and HITECH Acts - Understand training requirements</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Monitoring activities completed by HIPAA Compliance Officer.</td>
<td>- Policy review and updates - Walk-throughs - Audits</td>
</tr>
<tr>
<td>Walk-Through</td>
<td>Conduct walk-through of facilities.</td>
<td>- Oral communications - Work stations - Email, fax, printers, copy machines - Document storage and disposal - Handouts - Other issues</td>
</tr>
</tbody>
</table>

### HIPAA Monitoring Example

#### Specific scope areas and tests

<table>
<thead>
<tr>
<th>Scope Areas</th>
<th>Testing Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Confirm periodic review and update.</td>
</tr>
<tr>
<td>Training</td>
<td>Confirm review and update.</td>
</tr>
<tr>
<td>Business Associate contracts</td>
<td>Review business associate agreements, follow up on complaints.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Obtain and review a sample of completed authorizations for PHI.</td>
</tr>
<tr>
<td>Right of Access/Denial of Access</td>
<td>Obtain and review approved and denied access requests for a sample of individuals.</td>
</tr>
<tr>
<td>Complaints</td>
<td>Review a sample of complaints.</td>
</tr>
<tr>
<td>Whistleblowers</td>
<td>Review any whistleblower complaints and outcome of investigation.</td>
</tr>
</tbody>
</table>