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 projects and initiatives focused on ensuring compliance with 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.

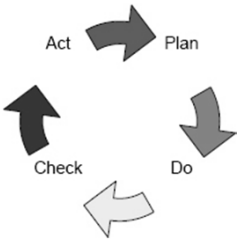
285 Mercer Street, 5th Floor
New York, NY 10003
Office: 212-992-8348
Mobile: 646-530-1931
Email: jessica.wasserman@nyu.edu

Essential Elements of an Effective Compliance Program

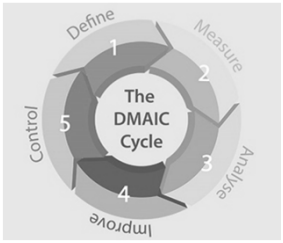
1. Establish policies, procedures and controls;
2. Exercise effective compliance oversight;
3. Exercise due diligence to avoid delegation of authority to unethical individuals;
4. Communicate and educate employees on the compliance program;
5. **Monitor and audit the compliance program for effectiveness;**
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.



Dr. W. Edwards Deming's PDCA



Six Sigma

ACMP/CCMP

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.

Ad Hoc	Check the Box	Committee Reporting	Active involvement
• Focus was on implementing a compliance program • Monitoring was reactive or came at request of management	• Identified list of compliance activities to monitor • Monitoring consisted of follow up with compliance risk owner	• Committee members identified compliance risks and tracked monitoring of risk for annual report to the Board	• Compliance team member prioritizes compliance risk areas • He/She helps identify key controls and conducts testing

Monitoring Framework

Pre-Framework

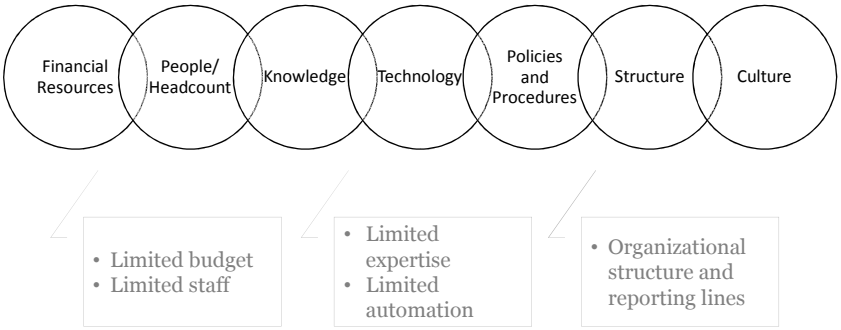
Before you dive into developing your monitoring framework, consider and ask yourself the following questions:

- 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?

Pre-Framework Activity

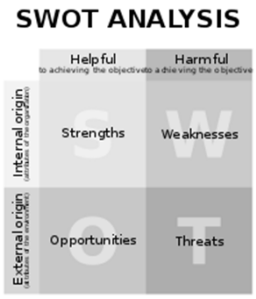
Constraints

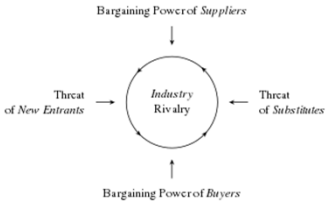
Below are some types of constraints that compliance functions may be subject to at higher education institutions.



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.

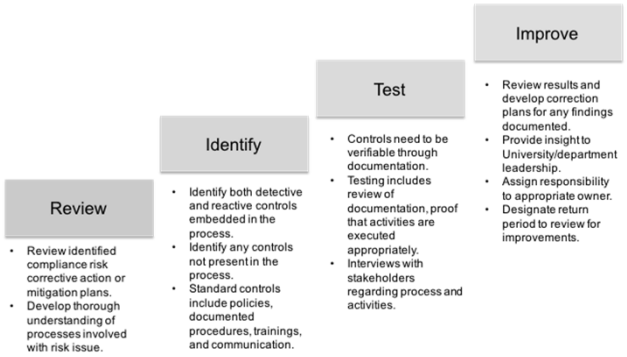
Assess	Develop	Execute	Review
• Legal and regulatory environment • Current risk or compliance monitoring practices	• Identify stakeholders and subject matter experts • Document processes and controls • Create monitor and test plan	• Conduct monitoring and testing activities • Document results • Communicate 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.

Risk Issue	Risk Score	Process Details
What is the compliance risk issue that has been identified?	What is the total risk score? A higher risk score may need more continuous monitoring.	Document the process to address the compliance risk. What is currently being done to address the risk? Need to know the whole process to identify controls.

Controls	Present or Future	Owners	Timeframe	Date	Findings
Controls come in all forms. Some most common ones include: Policies Documented processes Training System controls	Is the control already in place or is it still waiting to be implemented?	There should be an owner responsible for monitoring the control. Please note that a compliance process may have multiple owners.	How often will you test or review these controls?	Date of test or review	Findings should be viewed as constructive feedback. Time is provided to fix controls and processes. If there are controls deemed to costly or burdensome, a discussion with management can clarify how to proceed forward.

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.

Compliance Matter	Description and Tasks	Responsible Officer
September		
Higher Education Opportunity Act (HEOA)	Notification to students of Federal Student Financial Aid Penalties for Drug Law Violations; Copyright. All disclosures must be made concurrent with fall registration.	
HEOA – IPEDS Information	Complete and submit Integrated Postsecondary Education Data System (IPEDS) in a timely manner. Public information must be made available on nyu.edu.	
October		
FERPA	Each educational agency or institution shall annually notify students currently in attendance, of their rights under FERPA. Notification of these rights concurrent with fall registration is suggested, as the student needs to be told what information the student has identified as directory information and notified of his/her opportunity to place a hold on release of directory information. Notice is on website. Email will be sent out Spring semester.	
HIPAA	Monitor HIPAA compliance activities and requirements.	

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*

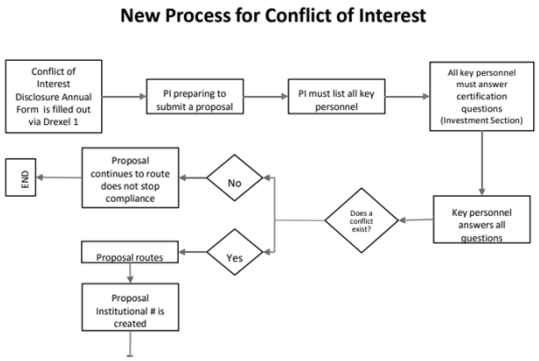
Please note that controls are not perfect and can fail due to various reasons like overrides, human or technology error, etc.

*Definitions borrowed from Gates Garrity-Rokous SCCE Higher Education Conference Session "Building an Institution-Focused Testing and Monitoring Program.

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

COI-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.

Case 2 - HEOA

Review and testing of controls

Scope Areas	Testing Activities (examples)
Availability of institutional information	• Confirm notices sent out regarding FERPA and information posted • Security and Fire Safety reports are available online • Facts and figures posted by Institutional Research
Availability of tuition, financial aid information and resources	• Confirm information regarding the cost of attending is available as well as access to the net price calculator.
Policies for transfer credits, refunds in case of withdrawal	• Check access to policies online. • Confirm they were reviewed and updated.
Provide NYU information on College Navigator website	• Confirm NYU information was reviewed, updated, and submitted to the Government's College Navigator website.
Financial Aid	• Confirm information regarding financial aid is accessible online. • Confirm policy on eligibility for financial aid was reviewed and updated. • Preferred lenders code of conduct?
Health & Safety	• Confirm statistics is published regarding alcohol and drug abuse violations. • Was policy reviewed, updated and published for both substance abuse and alcohol use and vaccinations.

Appendix

Resources

Higher Education Compliance Alliance

http://www.higheredcompliance.org/matrix/

http://www.higheredcompliance.org/about/

SCCE

http://www.corporatecompliance.org/Home.aspx

Check out SCCE resources – previous conference presentations on monitoring

Government

https://www.ed.gov/

Other

https://www.insidehighered.com/

List of Common Compliance Risk Areas – For Monitoring

HEA/HEOA	Environmental Health & Safety	Tax-exempt Bonds
Title IX	Research/Lab Safety	Clery Act/Campus Safety
Title IV	Conflicts of Interest	Financial Aid
Minors on Campus	Export Controls	Other Data and Privacy Requirements
GLBA	Human Resources (e.g., I-9)	Discrimination and Affirmative Action
HIPAA	Federal Grant Management	990 and 990T Reporting
FERPA	Bribery	Accreditation
"Red Flags"	Restricted Gifts	Completed Risk Projects
Reporting Line	Code of Conduct Review/Training	State & City Compliance Requirements

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 entities
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

Type	Action	Scope Areas (examples)
Policies	Review applicable policies and procedures.	• Uses and disclosures for PHI • Notice of Privacy Practices • Access PHI • Confidential communications • Accounting of PHI
Training	Review training and training requirements.	• Training provides overview of HIPAA and HITECH Acts • Understand training requirements
Monitoring	Understand what monitoring activities are completed by HIPAA Compliance Officer.	• Training monitoring • Policy review and updates • Walk-throughs • Audits
Walk-Through	Conduct walk-through of facilities.	• Oral communications • Work stations • Email, fax, printers, copy machines • Document storage and disposal • Handouts • Other devices

HIPAA Monitoring Example

Specific scope areas and tests

Scope Areas	Testing Activities (examples)
Policies and procedures	• Confirm periodic review and update. • Review to ensure coverage of HIPAA and HITECH requirements.
Training	• Sample training documentation (e.g., new hires, annual) • Confirm review and updates made to address regulatory changes
Business Associate contracts	• Obtain and review a sample of business associate agreements. Evaluate agreements.
Consent and authorizations for uses and disclosures	• Sample completed consents and authorizations
Verification requirements	• Obtain and review verification information for a sample of requestors of PHI.
Right of Access/Denial of Access	• Obtain and review approved and denied access requests for a sample of individuals.
Complaints	• Review a sample of complaints to covered entity.
Whistleblowers	• Review any whistleblower complaints and outcome of investigation.