Monitoring Mentor: Guidance for implementing a compliance monitoring program

Wednesday, June 7, 2017

SCCE Higher Education Compliance Conference

Jessica Wasserman, Asst Compliance Officer, New York University
John Powers, Manager, PwC

pwc

NYU

Outline

Introduction

Introduction - Bios

Jessica Wasserman is an experienced professional with a diverse business and operational background. Over the past 7+ 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.

John is a manager based in PwC's Chicago, IL office and works in the Internal Audit / Risk Assurance Practice. John has been working in public accounting since 2006, and has been with PwC since 2014.

John has worked in the higher education sector since 2011, serving in external audit, internal audit, and consultative roles. John has led comprehensive enterprise-wide risk assessments for large scale Universities and Academic Medical Centers, with a focus on strategic, financial, compliance, and operational risk. Since 2014, John has served as the lead internal audit manager on a full outsource engagement with a National Research University.
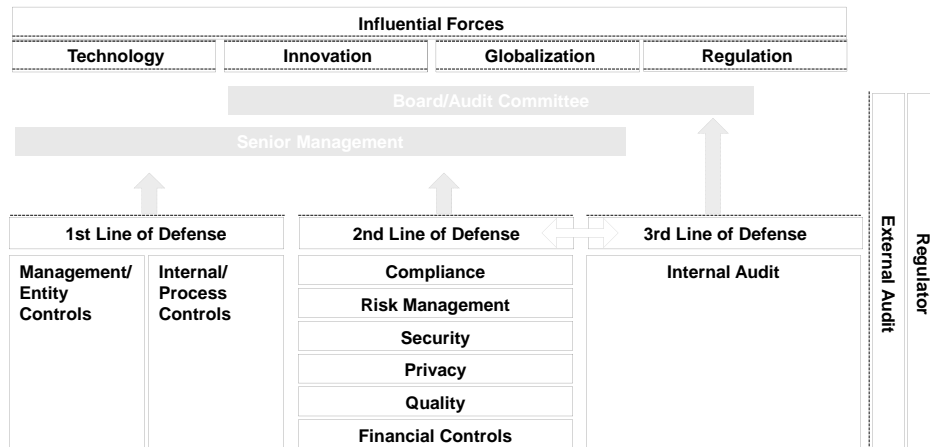
John has a B.B.S. from the University of Wisconsin-Madison in Risk Management and Insurance, and Accounting Information Systems. He is a Certified Public Accountant in the states of Illinois and Wisconsin.

Compliance Overview

5

7 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.

6

3

Three Lines of Defense

Influential Forces			
Technology	Innovation	Globalization	Regulation

Board/Audit Committee

Senior Management

1st Line of Defense		2nd Line of Defense	3rd Line of Defense	External Audit	Regulator
Management/ Entity Controls	Internal/ Process Controls	Compliance	Internal Audit		
		Risk Management			
		Security			
		Privacy			
		Quality			
		Financial Controls			

NYU & PwC

7

Common Compliance Risk Areas in Higher Education

Title IX – Sexual Misconduct & Athletics	Environmental Health & Safety	Research	Restricted gifts	990 and 990T reporting
Discrimination & Affirmative Action	Immigration	Institutional Review Boards	Laboratory Safety	Clery Act & Campus Safety
Federal awards management	International Activities & Programs	Institutional Reporting	Accreditation	Privacy & Security (HIPAA, FERPA)
Human Resources	Tax exempt bonds	Export Controls	Financial Aid	American with Disabilities Act

NYU & PwC

8

Current State of Compliance Monitoring in Higher Education

Before you assess your current compliance monitoring program ask yourself

1 What is the level of maturity & model of your risk and compliance program? (*Central / Decentralized*)

2 Do you need to improve the effectiveness of your monitoring and testing program to meet regulatory and/or stakeholder expectations?

3 How can you drive the optimization of your controls monitoring and/or reduce the costs of compliance?

4 Do you have the internal competencies, infrastructure, and subject matter expertise to drive an effective program?

5 How well do you use your data and technology to drive monitoring and testing activity and measure results across the Institution?

Current State: Common Compliance Structures

Strong Central Compliance Function

- Potential owners include Audit Services, Office of General Counsel, or an independent function;

- Has resources to conduct monitoring activities centrally under the direction of a CCO, may leverage the audit function or a cross functional compliance committee, may leverage external partners for subject matter expertise;

- Owns select compliance obligations (i.e., code of conduct, data privacy, investigations); **has defined compliance monitoring and periodic audits** for functional areas (i.e., research, athletics, financial aid); has line of sight relationships (i.e., business continuity); and,

- Has integrated technology into the function (i.e., data analytics, hotline, interactive website).

NYU & PwC

11

Current State: Common Compliance Structures

Strong Central Compliance Function

- Strengths
  - Clarifies ownership of key functions;
  - Has capacity to build monitoring and reporting for compliance functions that are not owned centrally; and
  - Can lead to a strong culture of compliance.
- Challenges
  - Most resource intensive to build and sustain;
  - If housed in General Counsel's Office may have a risk averse approach stifling innovation in maintaining compliance;
  - If housed in Audit Services may become overly investigative rather than collaborative; and,
  - An independent function may create conflict of interest with other central functions.

NYU & PwC

12

Current State: Common Compliance Structures

Hybrid Structure: Central Oversight, Local Ownership

- Generally led by a Compliance Steering Committee, possible presence of Vice President or Executive Director of Compliance;

- Central Oversight is designed to provide guidance/ serve in a consultative manner, standardizes goals, training, processes, policies, and enforcement;

- Lack of formal reporting relationships entails limited central ownership of select functions (i.e., written code of ethics/conduct, fraud hotline), and limited central monitoring of key risks due to resource constraints; and,

- Limited use of technology (i.e., hotline, landing page website).

NYU & PwC

13

Current State: Common Compliance Structures

Hybrid Structure: Central Oversight, Local Ownership

- Strengths
  - A functioning Steering Committee can rotate strategic topics, distributing the compliance workload among functional leaders;
  - Less resource intensive than a centralized model yet still allows for an opportunity to formalize compliance monitoring into a single source below the Board/Committee level.
- Challenges
  - Distributes workload onto functional leaders who may be limited in their efforts by capacity/bandwidth concerns;
  - Rotational aspect of the strategic topics presented at the Steering Committee assumes low turnover / stable environment to obtain the highest benefit of the model.

NYU & PwC

14

Current State: Common Compliance Structures

Decentralized Compliance Function

- Traditional & siloed environment, functional leaders own their compliance responsibilities and report to executive leadership, potential reactionary compliance environment led by Office of General Counsel;

- Organization requires functional leaders to monitor, remediate, and report upwards. Potential lack of common Institutional compliance goals, and limited accountability; and,

- Lack of technology for common compliance monitoring.

Current State: Common Compliance Structures

Decentralized Compliance Function

- Strengths
  - Least resource intensive;
  - Functional leaders are knowledge about their compliance responsibilities;
  - Accountability of compliance responsibilities is clear; and
  - No additional administrative burden or collaboration required.
- Challenges
  - Silos of compliance monitoring may create blind spots to senior leadership and the Board/Committees; and
  - May ultimately be more resource intensive than other models as functional leaders may build up local compliance functions in disproportionate manner compared to the risks of non-compliance to the organization.

Compliance Program Design Options
+ Leveraging Internal / External Partners

17

Constraints

Higher education organizations are faced with a number of constraints that play a part when designing a monitoring program.

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

- Limited budget
- Limited staff

- Limited expertise
- Limited automation

- Organizational structure and reporting lines
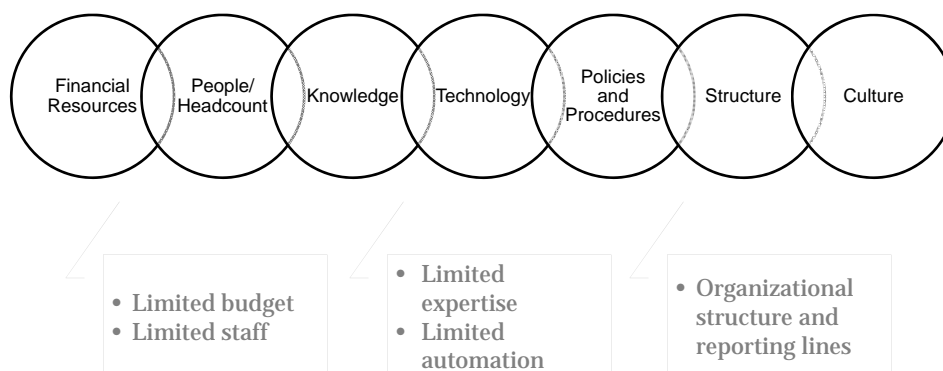
18

Centralized Compliance Function Design Option

Hybrid Compliance Function Design Option

Decentralized Compliance Function Design Option

Functional leaders are responsible for their respective compliance responsibilities & reporting is made primarily to regulators or within the function.

Board of
Trustees/
President

Requires:

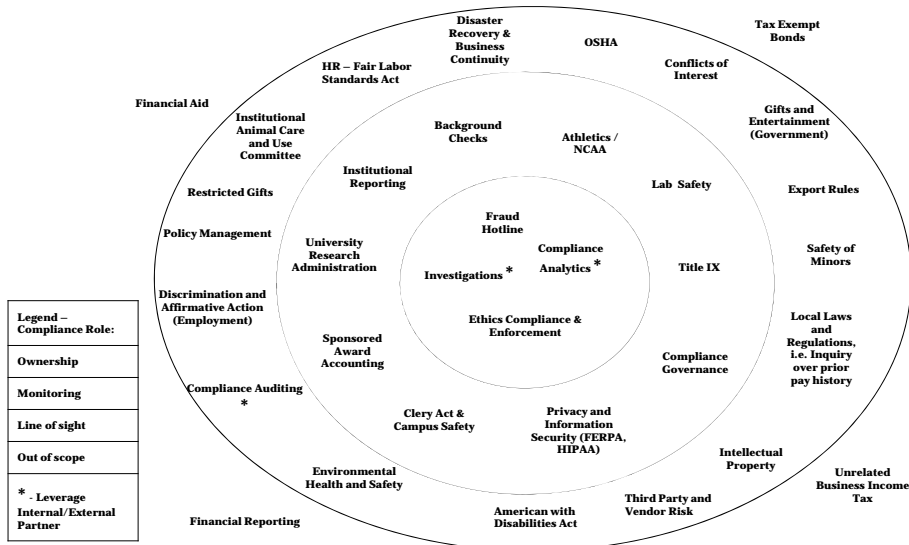- Culture of Accountability
- Knowledgeable Functional Leaders

NYU & PwC

21

Examples

1. A public university in the Northeast developed a questionnaire that it sends to compliance officers or other administrators who are affiliated with a particular compliance area. The questionnaire contains both standard and customized questions related to the compliance requirement.

2. Another university's compliance function rolls up to a VP in charge of internal audit, compliance, and risk management. The compliance function partners with the internal audit function to conduct compliance monitoring.

NYU & PwC

22

Implementation/Enhancement of your Compliance Monitoring Program

NYU & PwC

23

Action items to complete before implementing your monitoring program

- ☐ Determine what level of resources you have access to

- ☐ Inventory compliance requirement

- ☐ Identify processes and controls

- ☐ Research roles, ownership, requirements and resource expertise

- ☐ Determine reporting lines

- ☐ Speak to stakeholders

- ☐ Document your approach, methodology, schedule, key contacts and resources, processes and procedures

NYU & PwC

24

Implementation Example

A complex Organization migrating to a defined Centralized Compliance Function Bullseye:

1. Timing; Incubation to Maturity – Set milestones to manage risk

2. Resources allocated to the transition need to be knowledgeable, and time to transfer knowledge to the new owners of the compliance process. (*Leverage Internal & External Resources*)

3. Budget; consider resourcing and potential temporary duplication of efforts

4. Communication between the compliance function, the affected business unit, other impacted units, and relevant management.

NYU & PwC

25

Enhancement/Evolution Example

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

NYU & PwC

26

Examples and Ideas to Advance your Compliance Monitoring Program
+ Key Compliance Monitoring Activities & Controls

27

HIPAA 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

28

14

HIPAA Example

Review and Testing Controls – Part 1

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

NYU & PwC

29

HIPAA Example

Review and Testing Controls – Part 2

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.

NYU & PwC

30

Higher Education Opportunity Act (HEOA) Example

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.

NYU & PwC

31

HEOA Example

Review and testing of controls

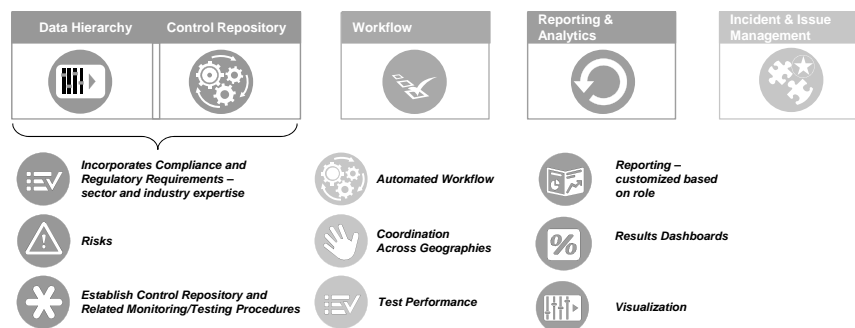| Scope Areas	Testing Activities (examples)
Availability of institutional information	• Confirm notices sent out regarding FERPA and information posted • Security and Fire Safety reports are available online • Facts and figures posted by Institutional Research
Availability of tuition, financial aid information 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.

NYU & PwC

32

16

Tools and Resources / Technology

Data Analytics: Using technology tools to enable and drive the sustainability of your program

A **technology tool** to support ongoing monitoring and testing should include the following key **elements** to provide efficiency and sustainability:

1. Knowledgeable users & an invested organizational culture

2. Interpreting and acting upon real time data, a compliance monitoring methodology that incorporates data analytics

3. Dynamic architecture/platform to respond to changing business risks

4. A defined reporting structure / distributed issues dashboard

Data Hierarchy	Control Repository	Workflow	Reporting & Analytics	Incident & Issue Management

Incorporates Compliance and Regulatory Requirements – sector and industry expertise

Automated Workflow

Reporting – customized based on role

Risks

Coordination Across Geographies

Results Dashboards

Establish Control Repository and Related Monitoring/Testing Procedures

Test Performance

Visualization

Advanced Monitoring and Testing to Enable Performance

Data analytics unlocks intelligence around compliance/controls performance

How does analytics enhance monitoring and testing programs?

Framework for evaluating areas for increased **automated testing** where feasible, increasing speed, effectiveness, and efficiency of testing

Manual testing executed with analytics, improving efficiency, and coverage; enhancing root cause identification

Mechanism for **intelligent sampling**/testing with 100% coverage

Intuitive dashboards enable continuous monitoring and real-time insight – using risk factors to slice, dice and **visualize** data to hone in on meaningful follow up activities

Advanced Monitoring and Testing to Enable Performance

February 26, 2016
35

Basic Data Analytics Example – T&E – Use of cash for gifts
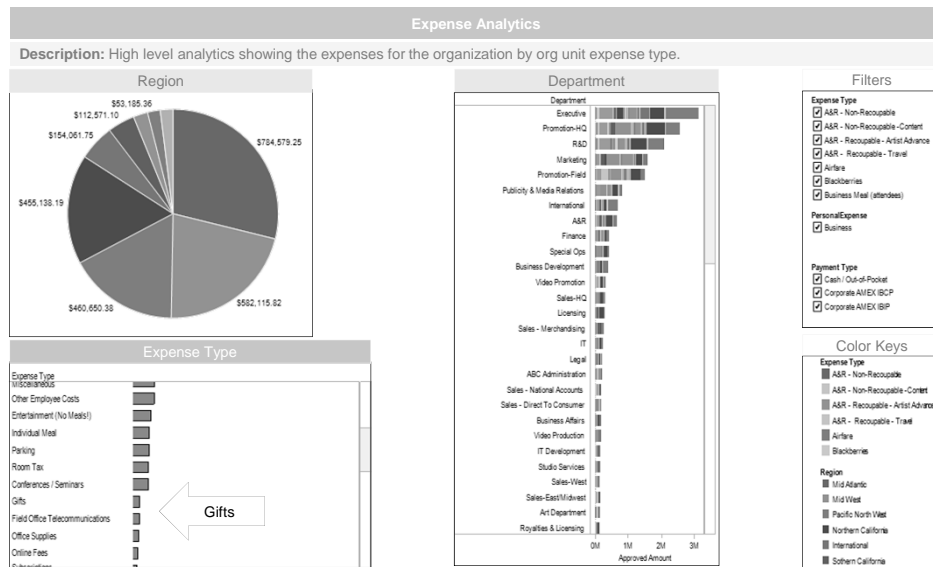
Advanced Monitoring and Testing to Enable Performance

February 26, 2016
36

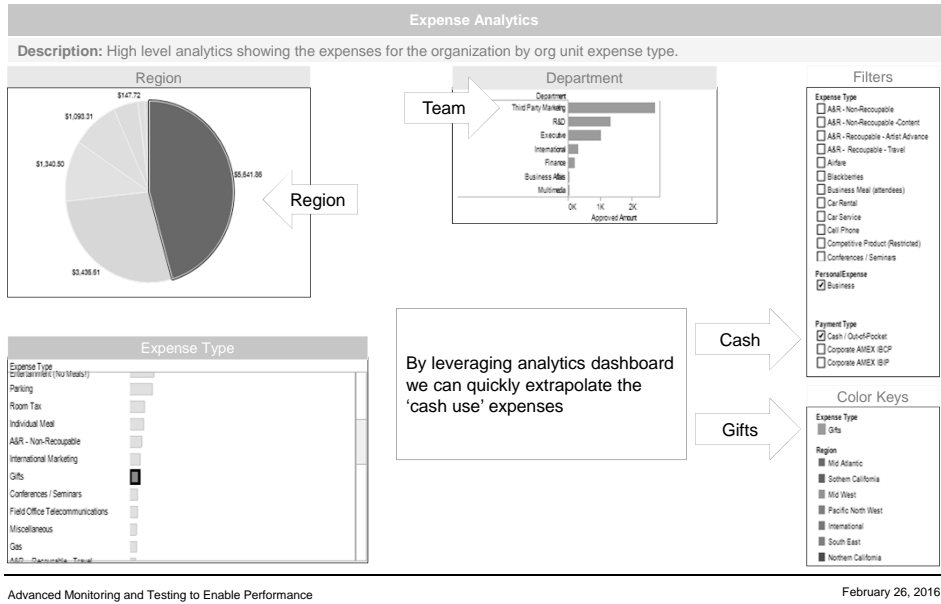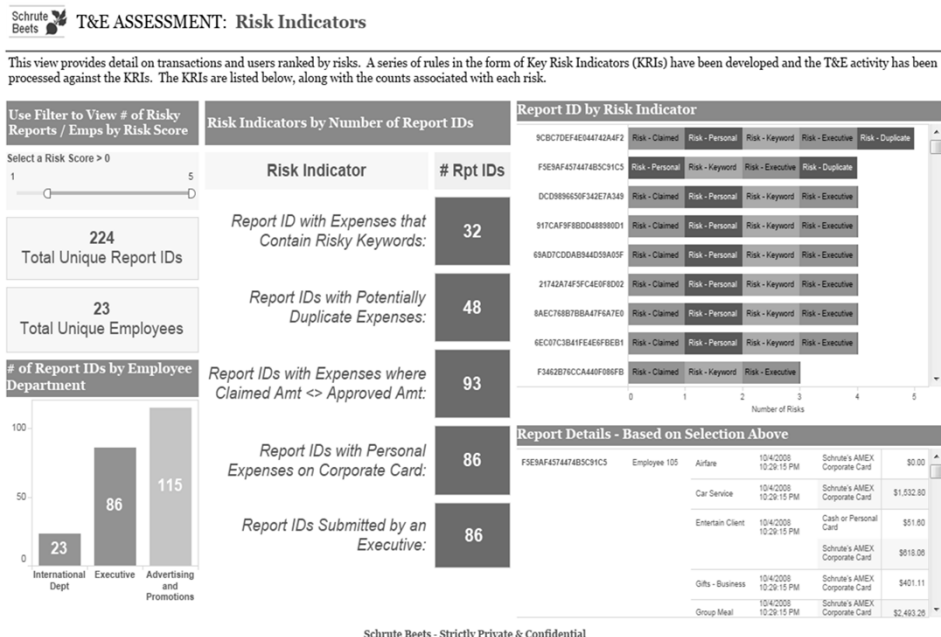## Basic Data Analytics Example – T&E – Use of cash for gifts *(continued)*

Tableau Data Visualization Example – Expense Report Monitoring, i.e. T&E Compliance – Athletics / Government

Common Technology Platforms/Systems

Data Visualization Resources
- *Useful for compliance activities that have significant amounts of data to organize*
  - Tableau
  - Qlikview
  - Microsoft Power BI

Governance Risk Compliance Resources
- *Useful for decentralized environments, policy/governance management, and IT compliance*
  - Archer
  - MetricStream
  - Bwise

NYU & PwC

39

List of Resources

Higher Education Compliance Alliance

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

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

SCCE

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

Government

https://www.ed.gov/

Other

https://www.insidehighered.com/

NYU & PwC

40

Thank you

Jessica Wasserman
Assistant Compliance Officer, Office of Compliance and Risk Management
New York University

285 Mercer Street, 5th Floor
New York, NY 10003
Office: 212-992-8348
Mobile: 917-536-5315
Email: jessica.wasserman@nyu.edu

John Powers
Manager, Risk Assurance
PricewaterhouseCoopers LLP

One North Wacker Drive
Chicago, IL 60606
Office: (312) 298-5058
Mobile: (608) 628-4162
Email: john.powers@pwc.com

NYU & PwC

41