

**MINNESOTA STATE COLLEGES AND UNIVERSITIES
BOARD OF TRUSTEES
Agenda Item Summary Sheet**

Name: Audit Committee

Date: May 21, 2014

Title: Review Results of Audit Risk Assessment

Purpose (check one):

Proposed
New Policy or
Amendment to
Existing Policy

Approvals
Required by
Policy

Other
Approvals

Monitoring /
Compliance

Information

Brief Description:

In June 2014, the Board of Trustees will be asked to approve the fiscal year 2015 audit plan. In preparation of that action, Audit Committee input is needed to determine priorities, given available resources and risk assessment results.

An audit risk assessment methodology was utilized to identify risks to consider in determining audit priorities for fiscal year 2015.

Professional internal auditing standards require that the audit plan be based on a risk assessment to ensure that resources are focused on the most critical projects.

Scheduled Presenter(s):

Beth Buse, Executive Director, Office of Internal Auditing
Eric Wion, Deputy Director, Office of Internal Auditing

**BOARD OF TRUSTEES
MINNESOTA STATE COLLEGES AND UNIVERSITIES**

BOARD INFORMATION
REVIEW RESULTS OF AUDIT RISK ASSESSMENT

1 **BACKGROUND**

2
3 The attached PowerPoint presentation documents the results of this work.

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35

36 *Date Presented to the Board of Trustees: May 21, 2014*

Minnesota State Colleges and Universities

Fiscal Year 2015 Audit Planning

Risk Assessment Results



Beth Buse, Executive Director, Internal Auditing

Eric Wion, Deputy Director, Internal Auditing


May 21, 2014

The Minnesota State Colleges and Universities system is an Equal Opportunity employer and educator.

Overview

- Internal auditing standards require that the audit plan be based on a documented risk assessment. The assessment must:
 - Consider input of senior management and the board
 - Take into account the organizations risk management framework
- Audit risk assessment methodology
 - Discussions with leadership
 - Review of Enterprise Risk Management study session results and discussions
 - Review of thought leadership on risks across sectors and specifically related to higher education
- Prioritization of Audit Resources
 - Financial Audits
 - IT Audits
 - Non-financial Operational Audits



Thought Leadership 


Books

Articles

White Papers

Case Studies

- Professional Organizations
 - Association of Governing Boards
 - Institute of Internal Auditors
 - Educause
 - ISACA
- Consulting firms
 - Deloitte
 - PWC
 - Gartner
 - Protiviti
 - Grant Thornton



3

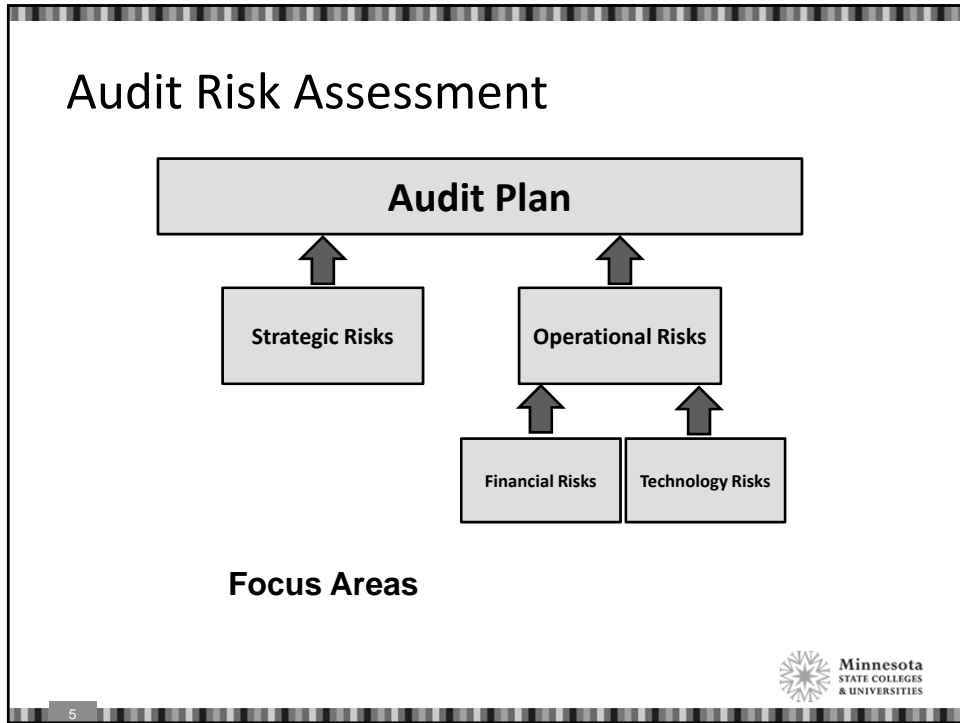
Thought Leader Themes Related to Risk



- Business transformation across all industries is a norm
- Cyber Security
- Social Media
- Affordable Care Act
- Reputational
- Higher Education - low enrollment and risk management



M

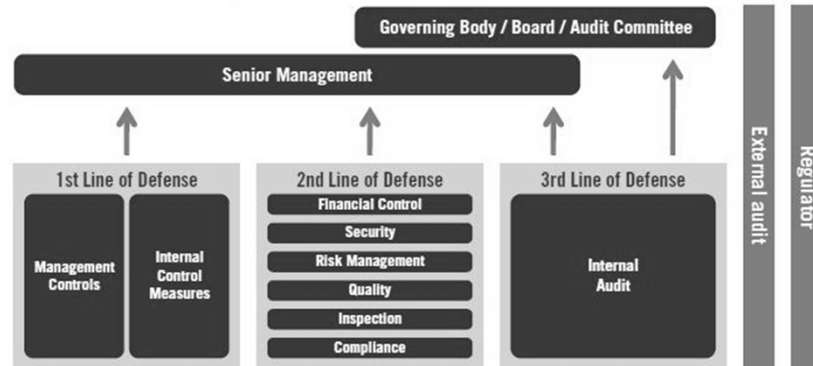
4



- 
- Strategic Framework – adopted by board in January 2012
 - Charting the Future – adopted November 2013
 - Implementation planning in progress
- 
- 6

Operational Risk Management

The Three Lines of Defense Model



Adapted from ECHIA/ERMA Guidance on the 8th EU Company Law Directive, article 41

Operational Risk Management: Three Lines of Defense Model

- First Line of Defense – functions that own and manage risks
 - Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives.
- Second Line of Defense – functions that oversee risks
 - Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls.
- Third Line of Defense – functions that provide independent assurance
 - Internal audit function

Operational Risks: Themes

- Overall: Resource constraint challenges
 - Impact and support of leadership transitions
 - Decentralized processes
 - Increasing complexity of operations and regulations
 - Encouraging innovation vs. implementing solutions on a systemwide basis
 - Limited second-line of defense
 - Energy and resources needed to implement change
 - Evolving risk management program



9

Operational Risks: Specific Topics

- Academic
 - International studies programs
 - Undergraduate student transfer
- Regulatory Compliance
 - Clery Act - Title IX
 - ADA - Environmental and Occupational Health and Safety
 - PCI
- Human resources
 - Pension administration
 - Workers compensation management



10

Operational Risks: Specific Topics

- Facilities
 - Keeping employees and students safe
 - Ability to effectively respond to emergencies
 - Deferred maintenance
- Other
 - Campus Service Cooperative
- Emerging
 - Affordable Care Act

Financial Risks



Background

- January 2014 – Board approved a revised financial audit plan for system
 - Reduced number of individual college and university audits
 - Goal to Increase number of financial internal control and compliance audits
 - Institution
 - Functional
- Risk Methodology
 - Institution risk model
 - Functional area analysis



13

Financial Risks: Institution

Metrics Used

Metric Category	Factors Measured
Audit (points = 350)	<ul style="list-style-type: none"> • Time since last internal control and compliance audit and the volume of findings • Whether the institution has an annual financial statement audit and the volume of findings from the last audit • Number of outstanding unsatisfactory audit findings
Financial Condition (points = 300)	<ul style="list-style-type: none"> • Operating gains or the size of losses • Composite Financial Index (CFI) • Overall materiality of financial transactions
Business Operations (points = 275)	<ul style="list-style-type: none"> • Change or loss in key personnel, knowledge, or skills • Diversity or complexity of operations • Number of incompatible security access rights
Other (points = 100)	Use of professional judgment to make or adjust for significant financial risks at a specific institution.

Total possible points = 1025

14

Financial Risks: Institution Risk Model Results

- Overall model showed increase in financial risk
 - Drivers
 - Increase in number of years since last internal control and compliance audit.
 - Over 10 years = 7
 - 6 – 10 years = 11
 - 0 – 5 years = 20
 - Increase in number of institutions with a negative net operating income (FY12 = 10 to FY13 = 20)
 - Decrease in CFI by 23 institutions from FY12 to FY13
 - Change in key personnel



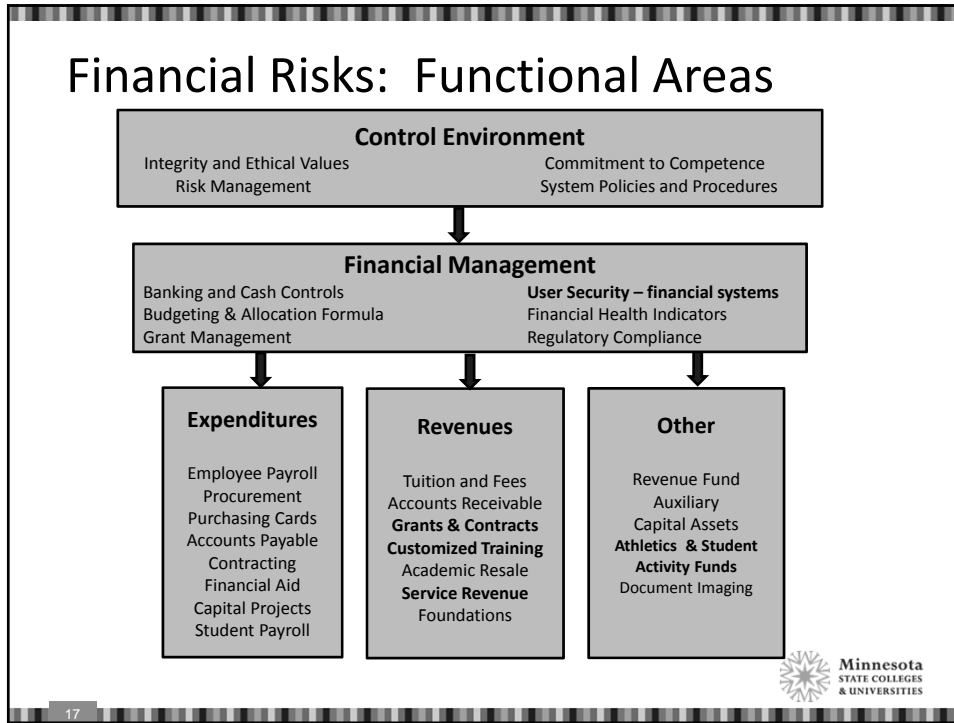
15

Financial Risks: Institution

- What should be the biggest factors in determining financial risk?
 - Materiality of financial transactions (size of institution)
 - Changing control (Loss of key personnel)
 - Time since last internal control and compliance audit
 - Other factors
- If materiality is biggest factor, does that mean no audits of smallest colleges?
- Should there be a required rotation?



16



- ## Financial Risks: Functional Areas
- ### Risk Assessment
- Internal Audit and Finance staff assessed risk
 - Risk considerations included
 - Materiality
 - Transaction volume and complexity
 - Susceptibility to Fraud
 - Compliance requirements
 - Past audit history
 - Individual High Risk Areas

<ul style="list-style-type: none"> ✓ Grant Management ✓ Employee business expense ✓ Tuition and fees ✓ Financial Aid ✓ Bookstore Operations 	<ul style="list-style-type: none"> ✓ Equipment Inventory ✓ Student Activity Funds ✓ Academic Resale Activities ✓ Capital Project Administration ✓ Banking and cash controls ✓ Purchasing cards
--	--
- Minnesota STATE COLLEGES & UNIVERSITIES
- 18

Information Technology (IT) Risks



Broad Categories of IT Risk

- **Confidentiality** – Private or not public data or system-reported information is protected from unauthorized disclosure or use
- **Integrity** – Data and system-reported information is complete and accurate
- **Availability** – Computer systems and data will be accessible (“up-and-running”) when needed

Cost of a Breach

- Reputation
- Education industry average cost per record is \$111*
 - Forensics consultants
 - Lawyer fees
 - Call centers
 - Websites
 - Mailings
 - Identity-protection and credit-check services
 - Additional security assessments and projects

* Source: Ponemon Institute report titled "2013 Cost of Data Breach Study: Global Analysis"



21

Breaches in Higher Education

- University of Maryland Data Breach (February 2014)
 - Over 300,000 student and employee records dating as far back as 1998
 - Cost is unknown – One expert estimates at least a couple million
- Indiana University (February 2014)
 - 146,000 student records exposed for 11 months because of an employee error
 - Known costs: \$75k for call center, \$6k on mailings & 700 hours of staff time
- North Dakota University (March 2014)
 - Over 291,000 student and employee records
 - Known costs include over \$200,000 on identity theft protection
- Maricopa County Community College District
 - 2.4M student, employee and vendor records going back 30 years
 - ~ \$10M notification, credit monitoring and remediation, \$2.7M legal fees, \$7M repair network and computers, likely class action lawsuit settlement unknown



22

Internal Audit - IT Risk Identification

- Discussions with IT professionals at the system office and some colleges and universities
- Attended annual MnSCU ITS conference
- Attended Regular Meetings: CIO Committee (biweekly), IT Risk Management Committee (monthly), and IT Guidelines Committee (monthly)
- Reviewed various documents
 - *IT Service Delivery Strategy* document
 - System Policies, Guidelines and Procedures
- Auditor brainstorming and input



23

MnSCU Computing Environment

- System office manages wide area network and mission critical enterprise technologies
 - Learning Management System (LMS)
 - Enterprise Resource Planning (ERP) system supports business functions including accounting, human resources, payroll, student registration, grades, transcripts and financial aid
 - Operational Data (Warehouse)
 - Vulnerability Management System (VMS)
 - Identity and Access Management (IAM) System



24

MnSCU Computing Environment

- Each college and university manages own data center(s), local area networks and other institution-specific info. Systems
 - Difficult for Internal Audit to determine
 - What we do know about Institution IT
 - Each responsible for managing/securing own networks, computers, and applications
 - Employees and students access enterprise systems
 - Commercial and custom applications are used
 - Many copy ISRS data and store it in local databases
 - Each have point-of-sale systems and process credit card transactions
 - Third-party outsourcing of some IT services



25

FY15 Audit Planning



26

FY15 Audit Planning

- Resource Prioritization
 - Financial
 - Individual College and University
 - Functional
 - Information Technology
 - Security
 - Operational
 - Compliance
 - Program areas



27

Questions

- Are there risk areas that we did not include that we should have?
- Given limited internal audit resources, what risks or risk areas should internal audit focus on in fiscal year 2015?
- Are there any other items that internal audit should take into consideration in planning the FY2015 audit plan?



28