MINNESOTA STATE COLLEGES AND UNIVERSITIES
BOARD OF TRUSTEES

Agenda Item Summary Sheet

Committee: Audit Committee **Date of Meeting:** June 19, 2013

Agenda Item: Review Results of Audit Risk Assessment, Including Information Technology Audit

□ Proposed Policy Change □ Approvals Required by Policy □ Other Approvals □ Monitoring

☒ Information

Cite policy requirement, or explain why item is on the Board agenda:

In June 2013, the Board of Trustees will be asked to approve the fiscal year 2014 audit plan. In preparation of that action, Audit Committee input is needed to determine priorities, given available resources and risk assessment results.

Scheduled Presenter(s):

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

Outline of Key Points/Policy Issues:

- A three-staged risk assessment was utilized to identify enterprise, financial, and information technology risks to consider in determining audit priorities for fiscal year 2014.

Background Information:

- 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.

BOARD OF TRUSTEES
MINNESOTA STATE COLLEGES AND UNIVERSITIES

INFORMATION ITEM

REVIEW RESULTS OF AUDIT RISK ASSESSMENT,
INCLUDING INFORMATION TECHNOLOGY AUDIT

A three-staged risk assessment identified enterprise, financial, and information technology risk factors. The attached PowerPoint presentation documents the results of this work.

Date Presented to the Board of Trustee: June 19, 2013

Minnesota State Colleges and Universities

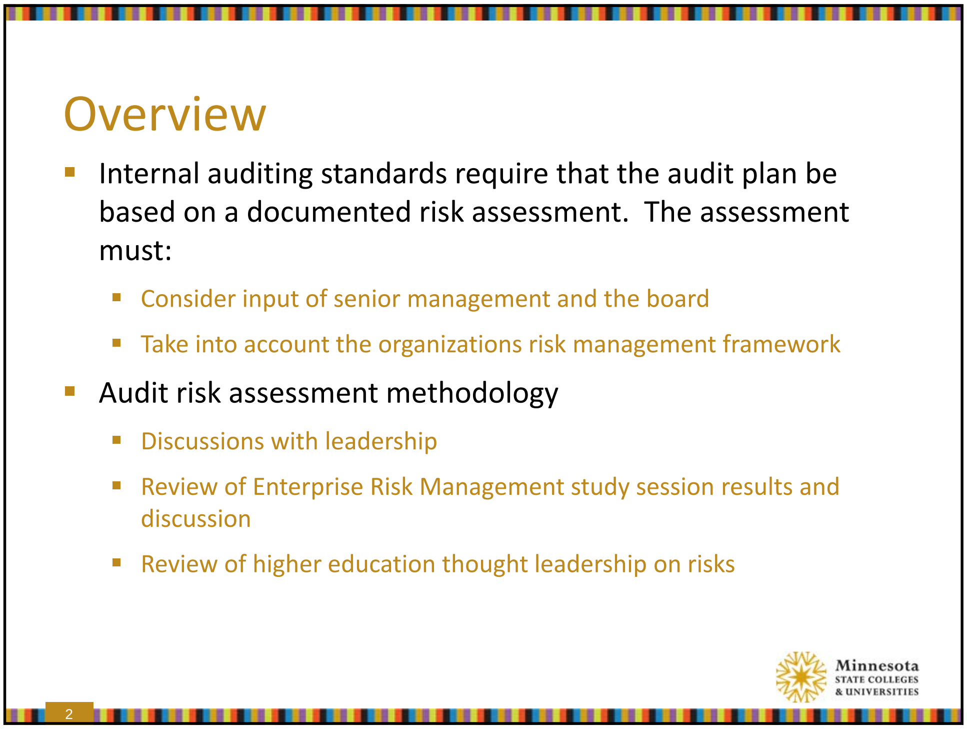
Fiscal Year 2014

Audit Risk Assessment Results

Beth Buse, Executive Director, Internal Auditing

Eric Wion, Deputy Director, Internal Auditing

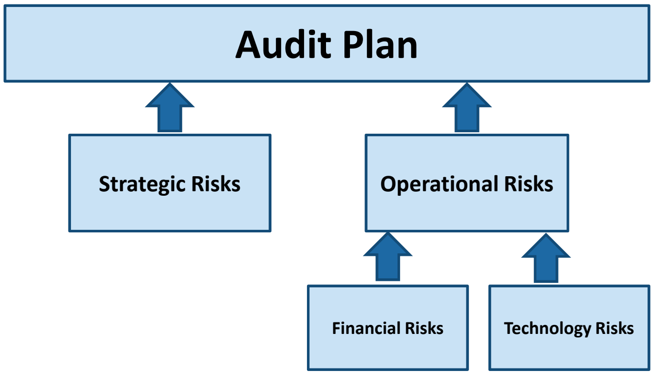
June 19, 2013



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 discussion
  - Review of higher education thought leadership on risks

Audit Risk Assessment



Audit Plan

Strategic Risks

Operational Risks

Financial Risks

Technology Risks

Focus Areas

Strategic Risks

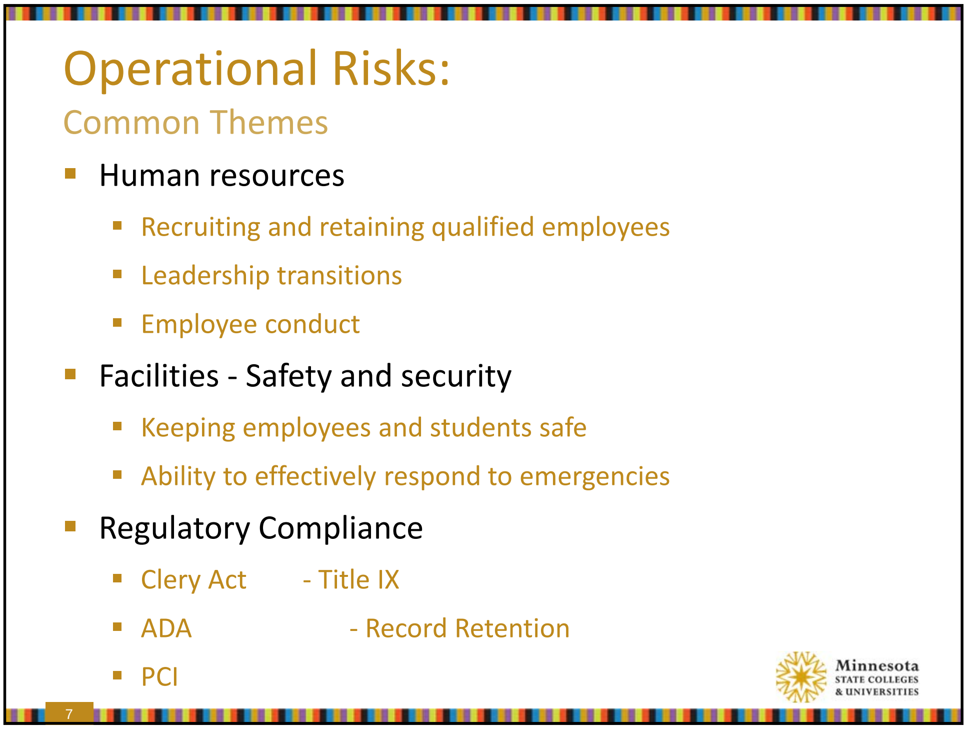
Strategic Risks

- Strategic Framework – adopted by board in January 2012
- Strategic Workgroups (Future of Higher Education, System of the Future, Workforce of the Future)
  - Draft strategies and recommendations to be presented in June 2013
  - Final report planned for fall 2013
  - Results could impact future internal audit projects
- Focus of May 2013 Enterprise Risk Management Study Session

Minnesota STATE COLLEGES & UNIVERSITIES

Operational Risks

Minnesota STATE COLLEGES & UNIVERSITIES

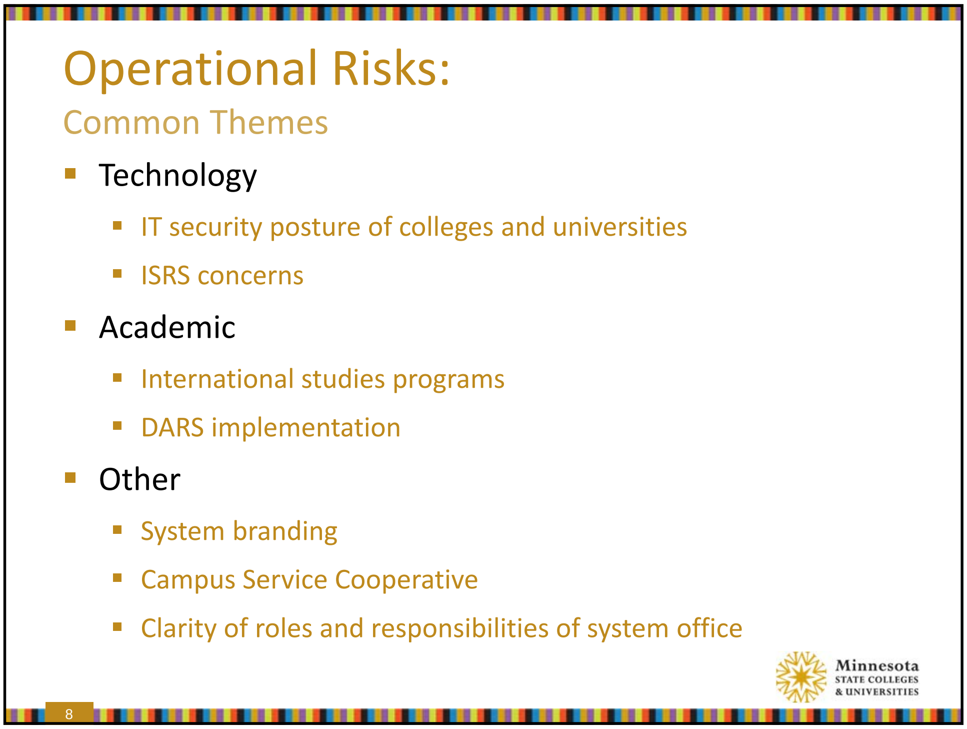


Operational Risks:

Common Themes

- Human resources
  - Recruiting and retaining qualified employees
  - Leadership transitions
  - Employee conduct
- Facilities - Safety and security
  - Keeping employees and students safe
  - Ability to effectively respond to emergencies
- Regulatory Compliance
  - Clery Act - Title IX
  - ADA - Record Retention
  - PCI

Minnesota STATE COLLEGES & UNIVERSITIES



Operational Risks:

Common Themes

- Technology
  - IT security posture of colleges and universities
  - ISRS concerns
- Academic
  - International studies programs
  - DARS implementation
- Other
  - System branding
  - Campus Service Cooperative
  - Clarity of roles and responsibilities of system office

Minnesota STATE COLLEGES & UNIVERSITIES

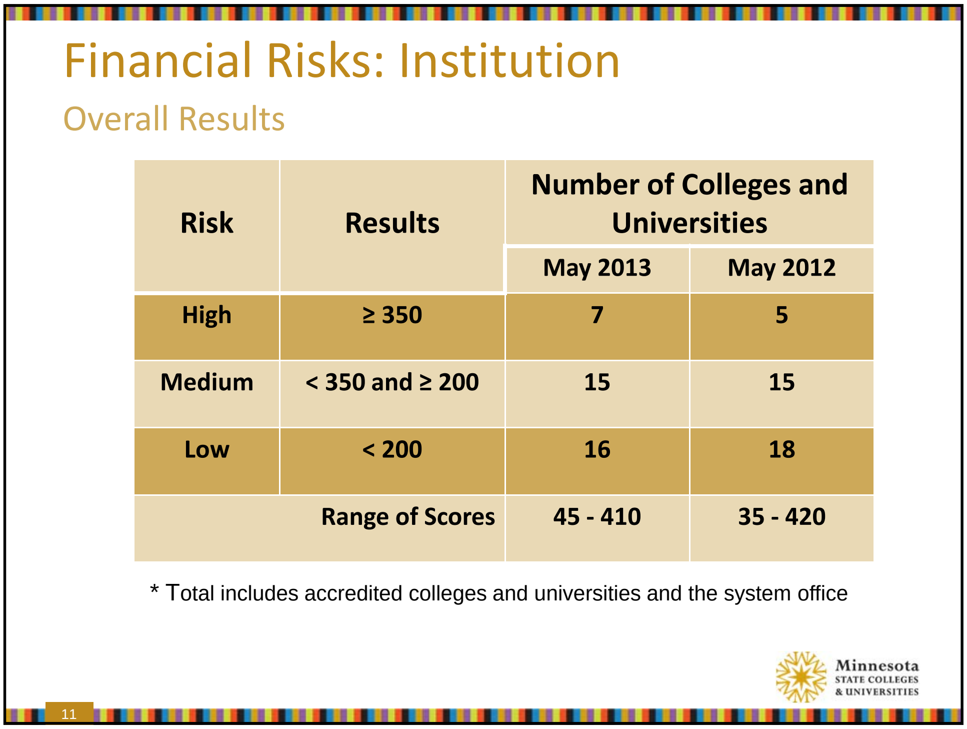
Financial Risks

Financial Risks: Institution

Metrics Used

Metric Category	Factors Measured
Audit (points = 350)	• 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)	• Operating gains or the size of losses • Composite Financial Index (CFI) • Overall materiality of financial transactions
Business Operations (points = 200)	• 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 = 950



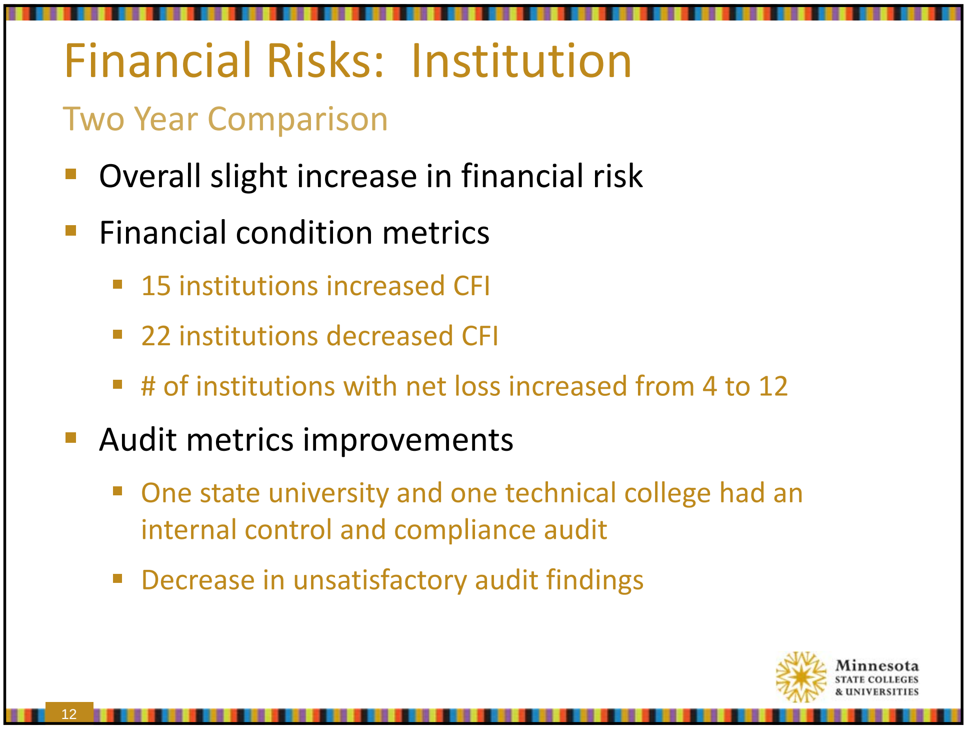
Financial Risks: Institution

Overall Results

Risk	Results	Number of Colleges and Universities	
		May 2013	May 2012
High	**≥ 350**	**7**	**5**
Medium	**< 350 and ≥ 200**	**15**	**15**
Low	**< 200**	**16**	**18**
	Range of Scores	**45 - 410**	**35 - 420**

* Total includes accredited colleges and universities and the system office

Minnesota State Colleges & Universities



Financial Risks: Institution

Two Year Comparison

- Overall slight increase in financial risk
- Financial condition metrics
  - 15 institutions increased CFI
  - 22 institutions decreased CFI
  - # of institutions with net loss increased from 4 to 12
- Audit metrics improvements
  - One state university and one technical college had an internal control and compliance audit
  - Decrease in unsatisfactory audit findings

Minnesota State Colleges & Universities

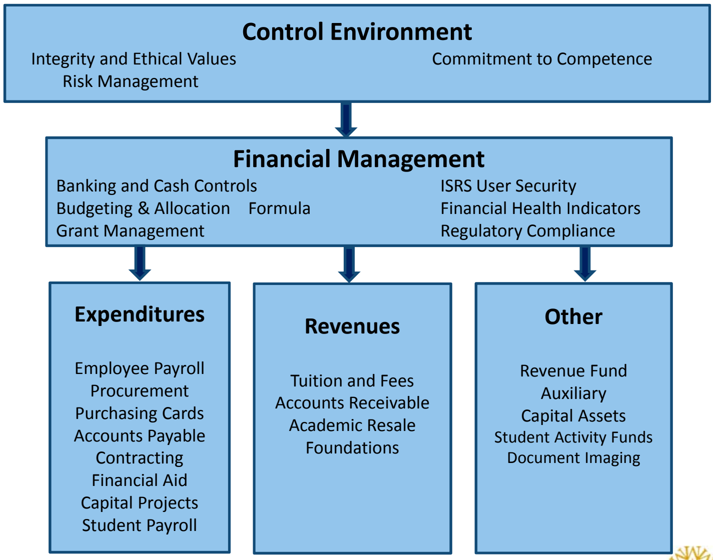
Financial Risks: Institution

Institutions with High Financial Risk

1. Southwest Minnesota State University
2. Winona State University
3. Minnesota State University Moorhead
4. Minneapolis Community & Technical College
5. Hennepin Technical College
6. Minnesota State University, Mankato
7. Dakota County Technical College

- Contributing Factors
  - Over ten years since last comprehensive internal control & compliance audit
  - Material financial activity
  - Complex operations
  - Large number of ISRS users with incompatible security access

Financial Risks: Functional Areas



Control Environment

Integrity and Ethical Values
Risk Management
Commitment to Competence

Financial Management

Banking and Cash Controls
Budgeting & Allocation Formula
Grant Management
ISRS User Security
Financial Health Indicators
Regulatory Compliance

Expenditures

Employee Payroll
Procurement
Purchasing Cards
Accounts Payable
Contracting
Financial Aid
Capital Projects
Student Payroll

Revenues

Tuition and Fees
Accounts Receivable
Academic Resale
Foundations

Other

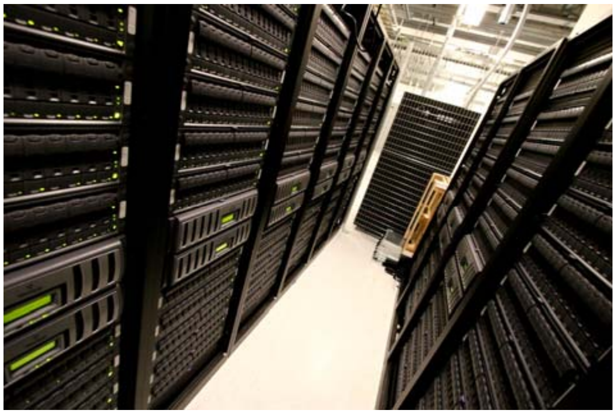
Revenue Fund
Auxiliary
Capital Assets
Student Activity Funds
Document Imaging

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
  - ✓ Grant Management
  - ✓ Employee business expense
  - ✓ Tuition and fees
  - ✓ Financial Aid
  - ✓ Bookstore Operations
  - ✓ Equipment Inventory
  - ✓ Student Activity Funds
  - ✓ Academic Resale Activities
  - ✓ Capital Project Administration
  - ✓ Banking and cash controls
  - ✓ Purchasing cards

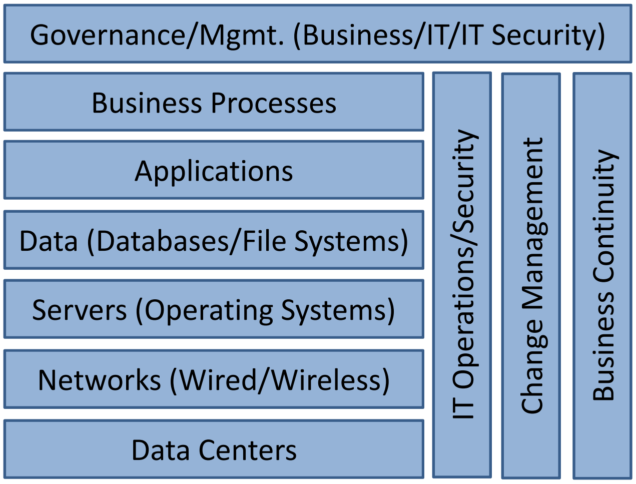
Information Technology (IT) Risks



Broad Categories of 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

Layers of Risks/Controls

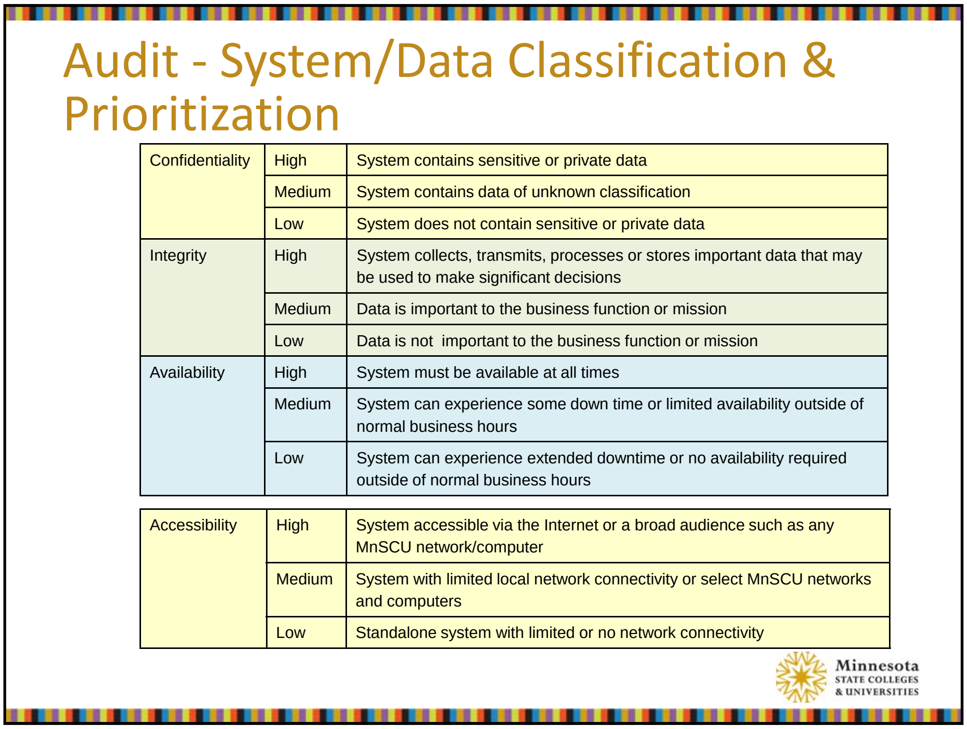

Governance/Mgmt. (Business/IT/IT Security)
Business Processes
Applications
Data (Databases/File Systems)
Servers (Operating Systems)
Networks (Wired/Wireless)
Data Centers
IT Operations/Security
Change Management
Business Continuity

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
  - Data Warehouse
  - Vulnerability Management System (VMS)
  - Identity and Access Management (IAM) System
- Each college and university manages own data center(s), local area networks and other institution-specific info. systems

Internal Audit - IT Risk Identification

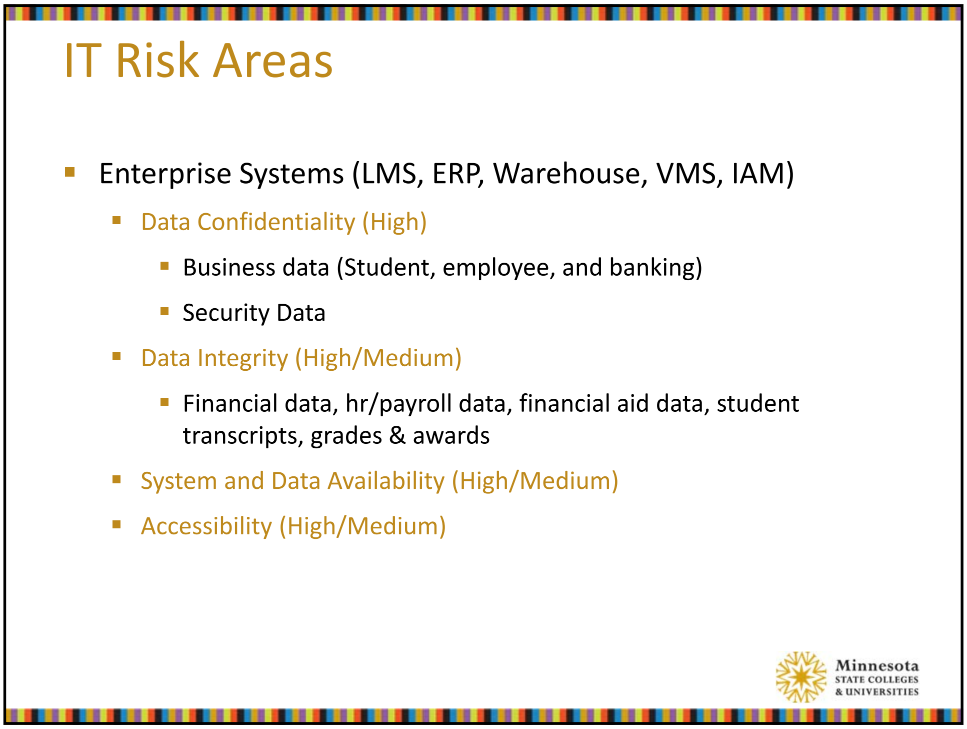
- Discussions with IT professionals at the system office and some colleges and universities
- Attended annual MnSCU ITS conference
- Attended bi-weekly CIO meetings and monthly Security Steering Committee meetings
- Reviewed various documents
  - *IT Service Delivery Strategy* document
  - System Policies, Guidelines and Procedures
- Auditor brainstorming and input



Audit - System/Data Classification & Prioritization

Confidentiality	High	System contains sensitive or private data
	Medium	System contains data of unknown classification
	Low	System does not contain sensitive or private data
Integrity	High	System collects, transmits, processes or stores important data that may be used to make significant decisions
	Medium	Data is important to the business function or mission
	Low	Data is not important to the business function or mission
Availability	High	System must be available at all times
	Medium	System can experience some down time or limited availability outside of normal business hours
	Low	System can experience extended downtime or no availability required outside of normal business hours

Accessibility	High	System accessible via the Internet or a broad audience such as any MnSCU network/computer
	Medium	System with limited local network connectivity or select MnSCU networks and computers
	Low	Standalone system with limited or no network connectivity



IT Risk Areas

- Enterprise Systems (LMS, ERP, Warehouse, VMS, IAM)
  - Data Confidentiality (High)
    - Business data (Student, employee, and banking)
    - Security Data
  - Data Integrity (High/Medium)
    - Financial data, hr/payroll data, financial aid data, student transcripts, grades & awards
  - System and Data Availability (High/Medium)
  - Accessibility (High/Medium)

IT Risk Areas

- Institution-Specific Systems
  - Difficult for Internal Audit to determine
  - What we do know about Institution IT
    - Each responsible for managing/securing own networks, computers, and applications
    - Commercial and custom applications are used
    - Many copy ISRS data and store it in databases
    - Employees and students access enterprise systems
    - Each have point-of-sale systems and process credit card transactions

Minnesota
STATE COLLEGES
& UNIVERSITIES