BOARD OF REGENTS
UNIVERSITY OF MINNESOTA

Audit Committee

December 2014

December 11, 2014

8:00 a.m. - 10:00 a.m.

East Committee Room, McNamara Alumni Center

AUD - DEC 2014

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **December 11, 2014**

Agenda Item: Institutional Risk Profile

☐ **Review** ☐ **Review + Action** ☐ **Action** ☒ **Discussion**

☐ *This is a report required by Board policy.*

Presenters: Regent Laura Brod
Gail Klatt, Associate Vice President

Purpose & Key Points

The purpose of this discussion is to review the Institutional Risk Profile. The profile is used to identify those risks of greatest import to the Board of Regents at a governance level. This profile is a synthesis of the committee's work in reviewing a broad range of risks identified by the administration over the last two years.

Background Information

At its February 11, 2011 meeting, the Board expressed support for the Strategic Risk Management Work Group's operational strategy and risk principles. These principles have provided a framework that has guided the University community toward a more strategic risk management approach to all aspects of its operations.

Over the past two academic years, the Audit Committee reviewed and discussed the risks associated with each of the major operational components of the University. Previous risk discussions by the committee include:

- Research (December 2012)
- Human Resources (February 2013)
- Information Technology (May 2013)
- University Operations (June 2013)
- Finance (September 2013)
- Intercollegiate Athletics (December 2013)
- Compliance (February 2014)
- Health Sciences (February 2014)
- Academics (May 2014)
- Research - *Updated* (June 2014)

The previous Institutional Risk Profile was last updated in 2009. The Audit Committee created the initial draft of the new profile at a work session on October 9, 2014.

University of Minnesota Institutional Risk Profile - Draft

The institutional risk profile is used to identify those risks of greatest import to the Board of Regents at a governance level. This profile is a synthesis of the committee's work in reviewing a broad range of risks identified by the administration over the last two years.

Likelihood	Low	Moderate	High
High	**G** • Campus Safety & Security	**D** • Athletics: Program Integrity & Success of Business Model • IT Infrastructure & Costs • Managing Brand & Reputation	**A** • Autonomy • Attracting & Retaining Talent • Data Privacy/Security • Student Demographics & Enrollment Strategies
Moderate	**H**	**E** • Maximizing Value of Multiple Campuses • Meeting Expectations on Workforce Development • Preparedness of Students • Public Perception of the Value of Higher Education	**B** • Facilities: Strategic Needs & Aging Infrastructure • Federal Research Funding • Higher Education Operating Model • Human Subjects Research • Implementation of Strategic Plans • Prioritization: Balancing Breadth & Quality of Offerings • State Funding • UM Health Success
Low	**I**	**F** • Commercialization of Intellectual Property	**C** • Effective Communication

Impact

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **December 11, 2014**

Agenda Item: External Auditor Report

☐ **Review** ☐ **Review + Action** ☐ **Action** ☒ **Discussion**

☒ *This is a report required by Board policy.*

Presenters: Michael Volna, Associate Vice President & Controller
Kirsten Vosen, Partner, Deloitte & Touche LLP
Judith Dockendorf, Senior Manager, Deloitte & Touche LLP

Purpose & Key Points

Deloitte will present the audit results for the FY 2014 annual financial report. Information presented by Deloitte will cover:

- The auditor's opinion on the University's financial statements.
- Significant accounting policies.
- Accounting estimates.
- Audit adjustments.
- Other required communications.

Background Information

The Audit Committee oversees external audit engagements on behalf of the Board of Regents. The FY 2014 financial report can be viewed in the December 12, 2014 Board docket.

Deloitte.

University of Minnesota

Presentation to the Audit Committee of the Board of Regents

Deloitte & Touche LLP
December 11, 2014 (information as of November 24, 2014)

Contents

Our professional standards require that we communicate with you concerning financial, accounting, and auditing matters that may be of interest to you in fulfilling your oversight fiduciary responsibilities. We have prepared the following comments to assist you in that regard.

Summary financial information

Consolidated Statements of Net Position (excluding component units)

(In thousands)

As of:	June 30, 2014	June 30, 2013	June 30, 2012
ASSETS			
Current assets	$ 589,977	$ 629,376	$ 585,161
Other noncurrent assets	2,231,939	2,040,048	1,971,938
Capital assets, net	2,900,494	2,876,914	2,696,951
Total assets and deferred outflows of resources	$ 5,722,410	$ 5,546,338	$ 5,254,050
LIABILITIES			
Current liabilities	$ 444,319	$ 443,100	$ 432,135
Noncurrent liabilities	208,518	184,726	167,583
Long-term debt	1,282,507	1,300,730	1,226,389
Total liabilities and deferred inflows of resources	$ 1,935,344	$ 1,928,556	$ 1,826,107
NET POSITION			
Unrestricted	$ 812,356	$ 820,146	$ 727,348
Restricted-expendable	1,004,191	865,819	784,443
Restricted-nonexpendable	289,366	277,601	265,156
Invested in capital assets, net of related debt	1,681,153	1,654,216	1,650,996
Total net position	$ 3,787,066	$ 3,617,782	$ 3,427,943
Total liabilities, deferred inflows of resources, and net position	$ 5,722,410	$ 5,546,338	$ 5,254,050

Consolidated Statements of Operations and Changes in Net Position (excluding component units)

(In thousands)

For the Year Ended:	June 30, 2014	June 30, 2013	June 30, 2012
Operating revenues	$ 2,093,360	$ 2,080,367	$ 2,068,917
Operating expenses	3,260,294	3,064,216	2,948,366
Operating loss	(1,166,934)	(983,849)	(879,449)
State and federal appropriations	633,863	597,530	587,220
Investment income, net	234,407	122,797	36,895
Capital appropriations	83,081	98,396	60,570
INCREASE IN NET POSITION	$ 169,284	$ 189,839	$ 124,701

Consolidated Statements of Cash Flows (excluding component units)

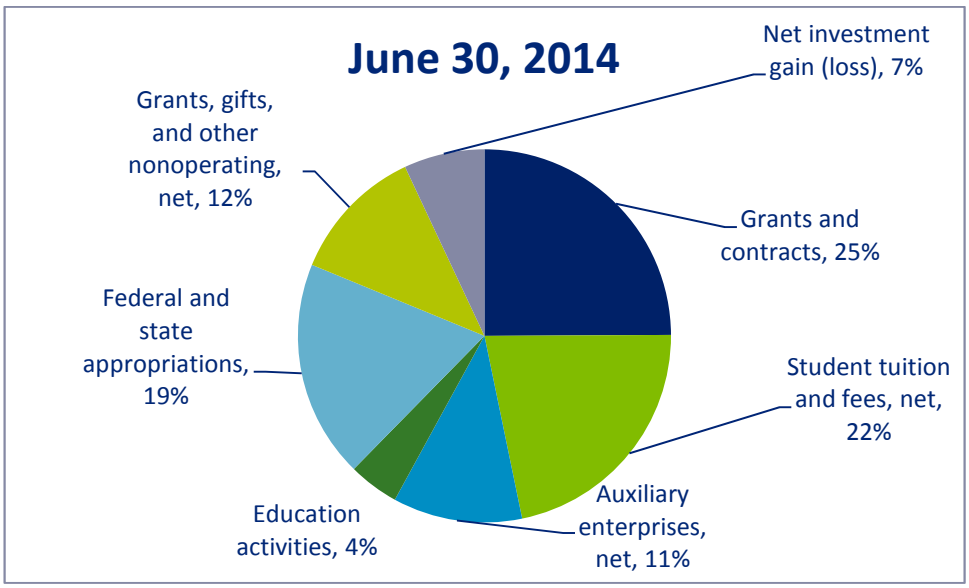
(In thousands)

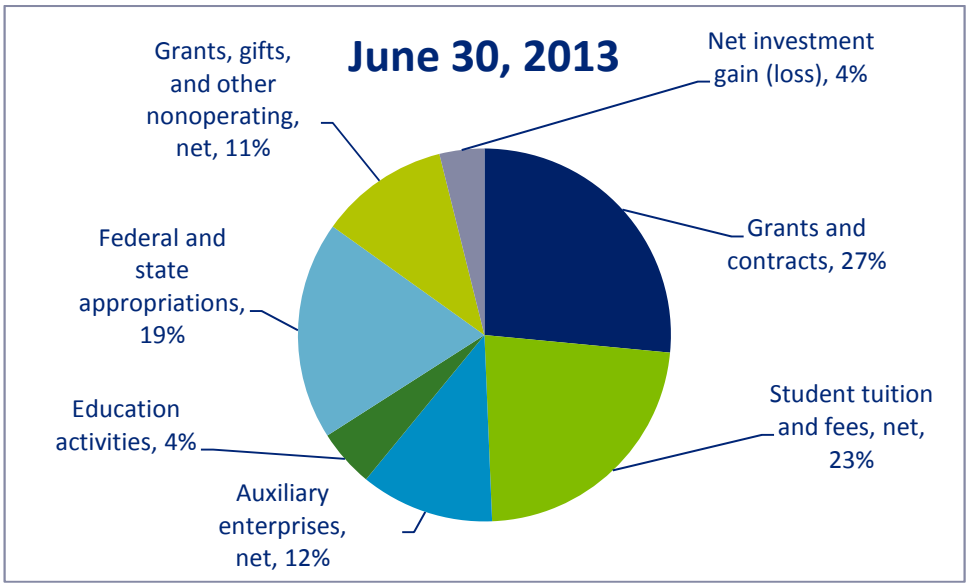
For the Year Ended:	June 30, 2014	June 30, 2013	June 30, 2012
Net cash used by operating activities	$ (924,284)	$ (781,600)	$ (659,788)
Net cash provided by non-capital financing activities	1,038,968	925,488	913,558
Net cash used by capital and related financing activities	(204,533)	(223,374)	(140,030)
Net cash provided by (used by) investing activities	118,775	4,977	(177,252)
Net increase (decrease) in cash	28,926	(74,509)	(63,512)
CASH — beginning of the year	281,011	355,520	419,032
CASH — end of the year	$ 309,937	$ 281,011	$ 355,520

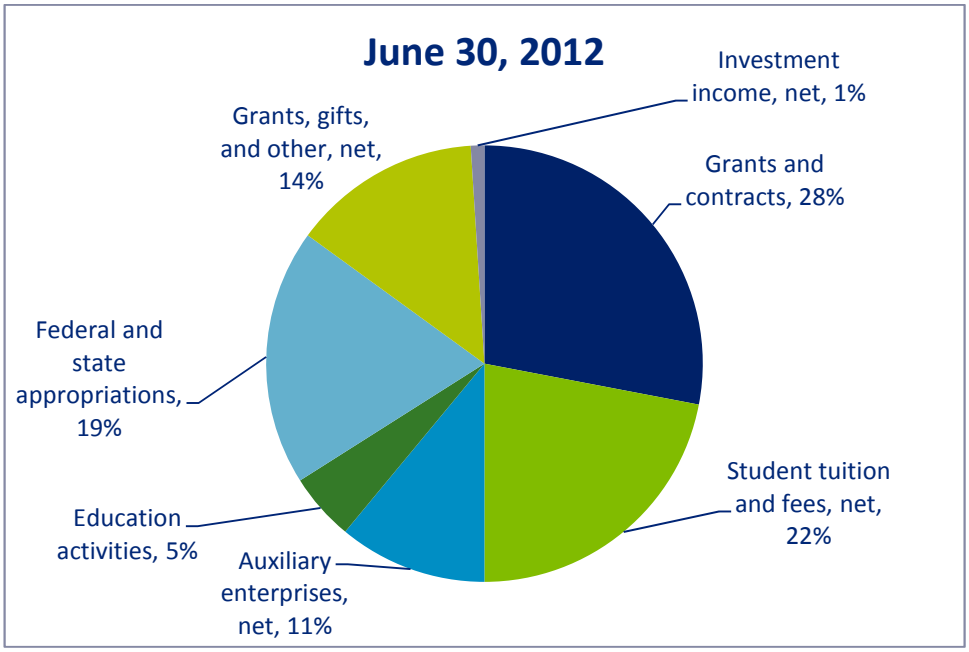
Enrollment Statistics

As of:	June 30, 2014	June 30, 2013	June 30, 2012
Approximate student enrollment	68,000	68,400	69,000

Total revenues






June 30, 2012
Investment income, net, 1%
Grants and contracts, 28%
Student tuition and fees, net, 22%
Auxiliary enterprises, net, 11%
Education activities, 5%
Federal and state appropriations, 19%
Grants, gifts, and other, net, 14%

Strengths, challenges and accomplishments of the University

Strengths of the University

- Ability and commitment to respond to changes, including new accounting pronouncements
- Strong accounting and finance functions
- Strong internal audit function with experienced professionals
- Research spending of $502 million benefits the entire state of Minnesota
- Diverse revenue base from tuition, state appropriations, federal grants, private gifts, grants, and contracts
- Strong net asset position
- Continued strong bond ratings (ability to generate additional funding)
  - Aa1 rating (Moody's-July 2014)
  - Strong market position for student demand and large research organization, growing balance sheet reserves and unrestricted balances, expendable financial resources provide favorable cushion of pro-forma debt, ample self-liquidity (per Moody's July 2014 report)
- Short and long term planning
- Long range capital planning
- Quality – ability to raise tuition and still have enrollment growth
- Strong endowment gains

Challenges faced by the University

- Erosion of public funding, particularly state appropriations, modest increase for FY 2014-2015 biennium
- Rising costs
- Need to continue to support infrastructure (annual depreciation of $192.7 million)
- Need for continued recruitment and retention of high-quality individuals within the finance and accounting departments
- Decentralization
- Large, complex systems upgrades are inherently challenging
- Challenges per Moody's report (July 2014)
  - Thinning operations and cash flows (lower operating cash flow margin) as well as challenges to growth in research funding due to federal funding environment and heightened competition

Accomplishments of the University

- Ability to respond to state funding shortfall while increasing graduation rates, increasing retention rates and increased first year student ACT scores
- Limited litigation exposure
- Minimal unrecorded audit adjustments
- Accounting Services met all significant audit deadlines and appears to have a strong desire to do what is right
- Successful bonding activity, solid bond ratings in the very strong category
- Risk Tolerance working group with formal presentations of risk heat maps to the Audit Committee

Required communications with the Audit Committee

Our Responsibility under Generally Accepted Auditing Standards and *Government Auditing Standards*

Our engagement letter dated May 27, 2014, described our responsibility under generally accepted auditing standards (GAAS) and *Government Auditing Standards* (GAS) including:

- To report whether, in our opinion, the consolidated financial statements are fairly stated in accordance with accounting principles generally accepted in the United States of America (GAAP) in all material respects
- To consider internal controls and assess control risk to the extent necessary to plan and perform audit procedures rather than to provide assurance on internal controls
- Our procedures are not designed specifically to detect fraud

We have completed our audit of the consolidated financial statements of the University of Minnesota (the "University") as of and for the year ended June 30, 2014. We have issued an unmodified opinion on the consolidated financial statements of the University.

We believe our audit fulfilled the objectives set forth in our engagement letter.

Internal controls

As described in our engagement letter, GAAS requires, among other things, that we obtain a sufficient understanding of the University's internal controls to enable us to properly plan our audit and to determine the nature, timing, and extent of our audit procedures to be performed. No observations or recommendations represent significant deficiencies or material weaknesses in internal controls for fiscal year 2014.

Significant accounting policies

The University's significant accounting policies are set forth in Note 1 to the 2014 consolidated financial statements.

The University adopted Government Accounting Standards Board Statement (GASB) No. 65, *Items Previously Reported as Assets and Liabilities* as of and for the year ended June 30, 2014 which resulted in $4.8 million in bond issuance costs that had previously been recorded as a prepaid expense on the consolidated statements of net position to be expensed in fiscal year 2014.

During the year ended June 30, 2014, there were no other significant changes in previously adopted accounting policies or their application.

Accounting estimates and key audit risks

Accounting estimates are an integral part of the consolidated financial statements prepared by management and are based on management's judgments. Those judgments are ordinarily based on knowledge and experience about past and current events and assumptions about future events.

Our conclusions as to the reasonableness of estimates, as expressed in our independent auditors' report, are based upon the testing of management's estimates and/or the development of an independent expectation of the estimates to corroborate management's estimates. Significant accounting estimates and key audit risks reflected in the 2014 consolidated financial statements include the following areas:

Summary of Accounting Estimates and Key Risks
• Valuation of investments and cash and cash equivalents • Long-term debt and Interest rate swaps • Recognition of revenue in the appropriate period • Information management and communication • Federal grant compliance

Financial Statement Account and 2014 $'s	Audit Procedures	Management's Assertions
Valuation of investments and cash and cash equivalents (Investments of $2.092 billion ($975 million considered alternative investments) and cash and cash equivalents of $244 million) (further breakout of investments included below)	• Read the valuations provided by external investment managers and management's year-end analysis to evaluate how positions are marked to market for a selected sample. Assessed the underlying assumptions used to determine fair value for alternative investment vehicles. • Updated our understanding of the University's investment portfolio and considered investment strategies or products that pose control or financial reporting risks. • Understood and documented the oversight and monitoring procedures performed by management when investing in new funds, quarterly and annually. • Obtained an understanding of the internal controls over the monitoring of and reporting on on-going invested funds. • Reviewed transactions at or near the balance sheet date which support the valuation of the investment. • Independently tested pricing of readily marketable investments. • Confirmed directly with external investment managers and requested related audited financial statements as required by American Institute of Certified Public Accountants guidance to verify underlying value of alternative investments for a selected sample. Performed rollforward procedures from audited financial statement date to June 30, 2014 for a selected sample. • Compared investment fund returns to standard industry benchmark for a selected sample.	Management has represented that the assumptions used are reflective of management's intent and ability to carry out specific courses of action and are consistent with the University's plan and past experiences. Also, these assumptions and methods used result in a fair value measure appropriate for financial statement disclosure purposes in accordance with GAAP.

Financial Statement Account and 2014 $'s	Audit Procedures	Management's Assertions
Interest rate swaps and long-term debt (Interest rate swaps notional amounts of $70 million and fair value of ($9.5) million) (Long-term debt of $1.283 billion)	• Confirmed long-term debt. • Assessed the University's compliance with debt covenants. • Obtained an understanding of all interest rate swap agreements. • Reviewed management's analysis and conclusion on accounting for interest rate swap agreements. • Assessed the financial condition of the interest rate swap counterparties.	Management has represented they have properly accounted for interest rate swap agreements, and that there are no negative financial conditions with any of the interest rate swap counterparties. Further, management has represented that the University is in compliance with all debt covenants as of June 30, 2014.
Recognition of revenue in the appropriate period (Student tuition and fees revenue of $732.8 million, net of allowance of $248 million) (Grant and contract revenue of $838.8 million) (Other operating revenue of $523.7 million, net of allowance of $9.5 million)	• Reviewed student tuition and fees and other revenue recognition accounting policies and procedures through our testing of internal controls • Audited student tuition and fees and other revenues recorded through substantive analytical and detailed testing procedures as well as testing completed within the federal grant compliance audit • Reconciled federal grant and contracts revenue with the federal grant compliance audit.	Management has represented that revenues have been recorded at the appropriate amounts and within the appropriate periods. Management has also represented that amounts recorded as federal grant and contracts revenue reconciles to revenues recorded within the federal grant compliance audit.
Information management and communication	• Utilized internal IT specialists to test and evaluate the computer-related controls within the business cycles, including revenue, expenditures, and payroll and personnel. • Performed internal control procedures around the University's ability to accumulate accurate and reliable information.	Management has represented that they have appropriate IT controls in place to produce accurate and reliable information to generate the consolidated financial statements.
Federal grant compliance (Federal and state grants of $1.067 billion)	• Understood compliance regulations applicable to the University's major federal programs as described in the U.S. Office of Management and Budget Circular A-133. • Held discussions with management, research leaders, and principal investigators and updated our understanding of procedures in place to comply with federal regulations. • Evaluated effort reporting costs charged to government grants in accordance with federal regulations. • Coordinated our tests for financial reporting purposes with our tests of compliance with government regulations. • Reviewed methodology and calculation used to determine indirect cost rate used by the University during the current fiscal year.	Management has represented that they have identified the requirements of laws, regulations, and the provisions of contracts and grant agreements that are considered to have a direct and material effect on each major federal program as identified in Part 3 of the Compliance Supplement dated March 2014. Also, management has represented that they have made available all information related to federal financial reports and claims for advances and reimbursements, which are supported by the books and records from which the consolidated financial statements have been prepared and are prepared on a basis consistent with that presented in the Schedule of Expenditures of Federal Awards.

Investments detail

(In thousands)

	Temporary Investment Pool	Consolidated Endowment Fund	Group Income Pool	Separately Invested Funds	RUMINCO	Total
Fixed income	$805,992	$211,651	$43,485		$13,478	$1,074,606
Public equity		390,831			25,337	416,168
Private capital		365,253				365,253
Inflation hedges		198,132				198,132
Other		21,014		$16,545		37,559
Total investments	$ 805,992	$1,186,881	$43,485	$16,545	$38,815	$2,091,718

During the year ended June 30, 2014, we are not aware of any significant changes in accounting estimates or in management's judgments relating to such estimates.

Audit adjustments

Our audit was designed to obtain reasonable, rather than absolute, assurance about whether the consolidated financial statements are free of material misstatement, whether caused by error or fraud. In addition, we are obligated by GAAS to inform you of any adjustments arising from the audit that could, in our judgment, either individually or in the aggregate, have a significant effect on the University's financial reporting process. There were no uncorrected misstatements, material corrected misstatements, or disclosure items passed that were identified during our audit.

Disagreements with management

We have not had any disagreements with management related to matters that are material to the University's 2014 consolidated financial statements.

Our views about significant matters that were the subject of consultation with other accountants

We are not aware of any consultations that management may have had with other accountants about auditing and accounting matters during 2014.

Significant findings or issues discussed, or subject of correspondence, with management prior to our retention

Throughout the year, routine discussions were held, or were the subject of correspondence, with management regarding the application of accounting principles or auditing standards in connection with transactions that have occurred, transactions that are contemplated, or reassessment of current circumstances. In our judgment, such discussions or correspondence were not held in connection with our retention as auditors.

Significant difficulties encountered in performing the audit

In our judgment, we received the full cooperation of the University's management and staff and had unrestricted access to the University's senior management in the performance of our audit.

Management representations

We have made specific inquiries of the University's management about the representations embodied in the consolidated financial statements. Management provided to us the written representations the University is required to provide to its independent auditors under generally accepted auditing standards.

Other matter paragraph

Our opinion on the consolidated financial statements includes an other matter paragraph specific to the required supplementary information that is included in the consolidated financial statements. Our opinion was not modified with respect to this matter.

Other findings or issues

There are no other findings or issues arising from the 2014 audit that are, in our professional judgment, significant and relevant to those charged with governance, regarding their oversight of the financial reporting process.

Other information in the Annual Report

The audited consolidated financial statements are included in the University's 2014 Annual Report. We read the other information in the University's 2014 Annual Report and inquired as to the methods and presentation of such information. We did not note any material inconsistencies or obtain knowledge of a material misstatement of fact in the other information.

Communication of peer review results

Peer Review

Deloitte participates in the American Institute of Certified Public Accountants (AICPA) Peer Review Program. The AICPA Peer Review Program requires independent evaluation every three years of those portions of a firm's accounting and auditing practice that are not inspected by the PCAOB (i.e., the non-SEC issuer practice) so firms can meet their state licensing, federal regulatory, and AICPA membership requirements.

In 2012, Ernst & Young LLP (E&Y) completed its most-recent triennial peer review of Deloitte & Touche LLP's system of quality control for our accounting and auditing practice applicable to non-SEC issuers for the year ended March 31, 2011. E&Y issued a report with a peer review rating of pass with deficiency, and included in its report a recommendation that D&T review the specificity of certain policies and procedures, implemented in connection with the adoption of a new audit methodology, to improve the consistency of audit execution and documentation.

We use all observations from our internal and external inspections to continuously improve audit performance, and have implemented enhancements to our audit policies and procedures that are responsive to the recommendation. The peer review report and our related response can be found at https://peerreview.aicpa.org/publicfile/Popup.aspx?f=10016352&r=320244&t=REV&s=1&e=.pdf.

Grant Thornton LLP has commenced the next triennial peer review of Deloitte & Touche LLP's system of quality control for our accounting and auditing practice applicable to non-SEC issuers for the year ended March 31, 2014. As of the date of this presentation, the peer review is not complete.

Information technology control procedures

- We deployed information technology controls specialists as part of our financial statement audit procedures to test general information technology controls related to the following critical financial reporting systems:
  - PeopleSoft Campus Solutions
  - PeopleSoft Human Resource Management System
  - PeopleSoft Enterprise Financial Systems
- We performed procedures to gain a detailed understanding of Information Technology (IT) controls related to core areas considered part of the financial audit framework of controls over financial reporting. The areas reviewed were Information Security, Data Center Operations, and System Change Control.

As a result of these procedures:

- We noted no findings or observations that represent significant deficiencies or material weaknesses in internal controls.

Summary of other 2014 audit services

A-133 Single Audit

- Testing is focused on Research and Development and Student Financial Assistance, two of the major federal programs at the University.
- Four additional programs were tested as major programs for the year ended June 30, 2014.
- Audit testing complete. Report issuance planned for December 2014.
  - To date, no findings noted.
- Federal expenditures for the year ended June 30, 2014 (in thousands):

Research and Development programs	$ 502,000
Student Financial Assistance programs	456,000
Other programs	109,000
Total Federal Expenditures	$ 1,067,000

Minnesota Office of Higher Education Financial Aid Programs examination

In connection with our procedures around the student financial assistance programs within the federal compliance audit, we performed procedures around the examination of the University's compliance with the Minnesota Office of Higher Education Financial Aid Programs requirements. We anticipate issuing our examination report in December 2014.

Student fees agreed-upon procedures

Agreed-upon procedures for 24 student organizations, as outlined by the Fees Committee and Office of Student Affairs, to assist in review of financial affairs and accounting records of student organizations. We anticipate issuance of agreed-upon procedures reports for each student organization in January 2015.

NCAA agreed-upon procedures

Agreed-upon procedures of the accounting records of the University of Minnesota Athletic Department in accordance with the NCAA Constitution. Procedures were performed in September 2014, with anticipated issuance of the agreed-upon procedures report in December 2014.

Other material written communications

- Written communications that we believe constitute other material written communications between management and us related to the audit for the year ended June 30, 2014, include:
  - Audit engagement letter — previously provided
  - Management representation letter (available upon request).

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **December 11, 2014**

Agenda Item: University of Minnesota Data Security Strategy

☐ **Review** ☐ **Review + Action** ☐ **Action** ☒ **Discussion**

☐ *This is a report required by Board policy.*

Presenters: Scott Studham, Vice President and Chief Information Officer
Brian Dahlin, Chief Information Security Officer

Purpose & Key Points

This is the second in a series of three discussions planned for FY 2015 regarding information security at the University of Minnesota. The purpose is to educate committee members about the University's approach to information security risk management and to support the Board's fiduciary oversight of the Office of Information Technology's security policies and programs. The series is designed to build a common understanding of issues and practices so committee members can develop a point of view concerning risk tolerance, as well as consider the cultural cost/benefit tradeoffs inherent in investing in additional efforts to mature our information security framework.

The first discussion highlighted the types of adversaries and threats in the current environment. The types of incidents encountered at the University were also discussed. That presentation additionally examined several high-profile incidents at peer institutions and elsewhere in the public sector.

This second discussion will provide a comprehensive overview of the University's information security framework and how it is positioned to mitigate the types of risks we are likely to encounter. The presentation also will provide an overview and assessment of the maturity of the University's information security framework, policies and practices, and risk management program.

Background Information

In May 2013, the Audit Committee discussed the University's data security framework, which is one component of the overall information security program. At the time, the University was transitioning from a two-tier data security classification (public vs. private) to a three-tier system that acknowledges different types of private data have different levels of associated risk and benefit from tailored controls. The first discussion in this series took place at the September 2014 meeting.

INFORMATION TECHNOLOGY

Information Security Overview
Audit Committee

Scott Studham
Vice President,
Chief Information Officer

Brian Dahlin
Chief Information
Security Officer

December 11, 2014

UNIVERSITY OF MINNESOTA
Driven to Discover℠

IT@UMN

A REFRESHER: INFORMATION SECURITY PRESENTATIONS

September - Information Security Primer

- ✓ What motivates “The Hacker?”
- ✓ Awareness of peer institutions
- ✓ Review recent examples (Target, higher ed, etc.)

December - Information Security Program Overview

- ✓ Information Security Program and Status
- ✓ Policy Standards and Risk Assessments

May – Discussion About Risk Profile

- ✓ Discuss information security assessment
- ✓ Consider framework component maturity levels

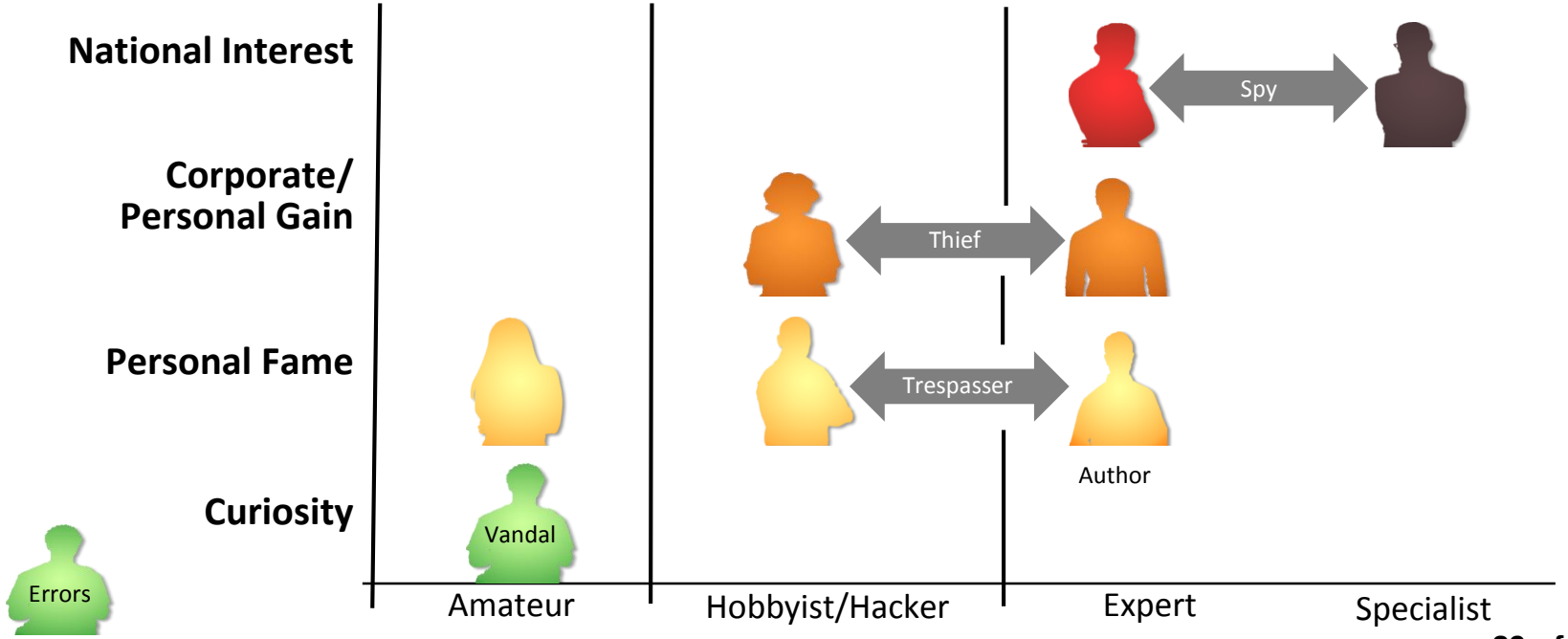
IT@UMN

“We in IT!”

Together with our partners across the University, we are aligning IT functions and teams to deliver the technology solutions necessary to advance the teaching, research and outreach missions of the University of Minnesota.

IT@UMN

What motivates an adversary?



IT@UMN

The language of information security – What we mean when we say…

Information Security Framework

The foundation for the structure of how the University's information security is organized. The framework includes components for program governance, security policy and standards, security risk management and exception management.

Security Standard

The detailed security rules that support the security policy and provide the specific expectations for the controls that must be implemented to meet the security policy.

Implemented Security Controls

The specific technical or procedural methods put in place to meet the security standards.

Security Risk Management

The process of evaluation that determines the risk of gaps in security standards and the risks related to unimplemented security controls. The security risk management process is the essential tool to balance security risk with other organizational risks and to prioritize implementation of security controls.

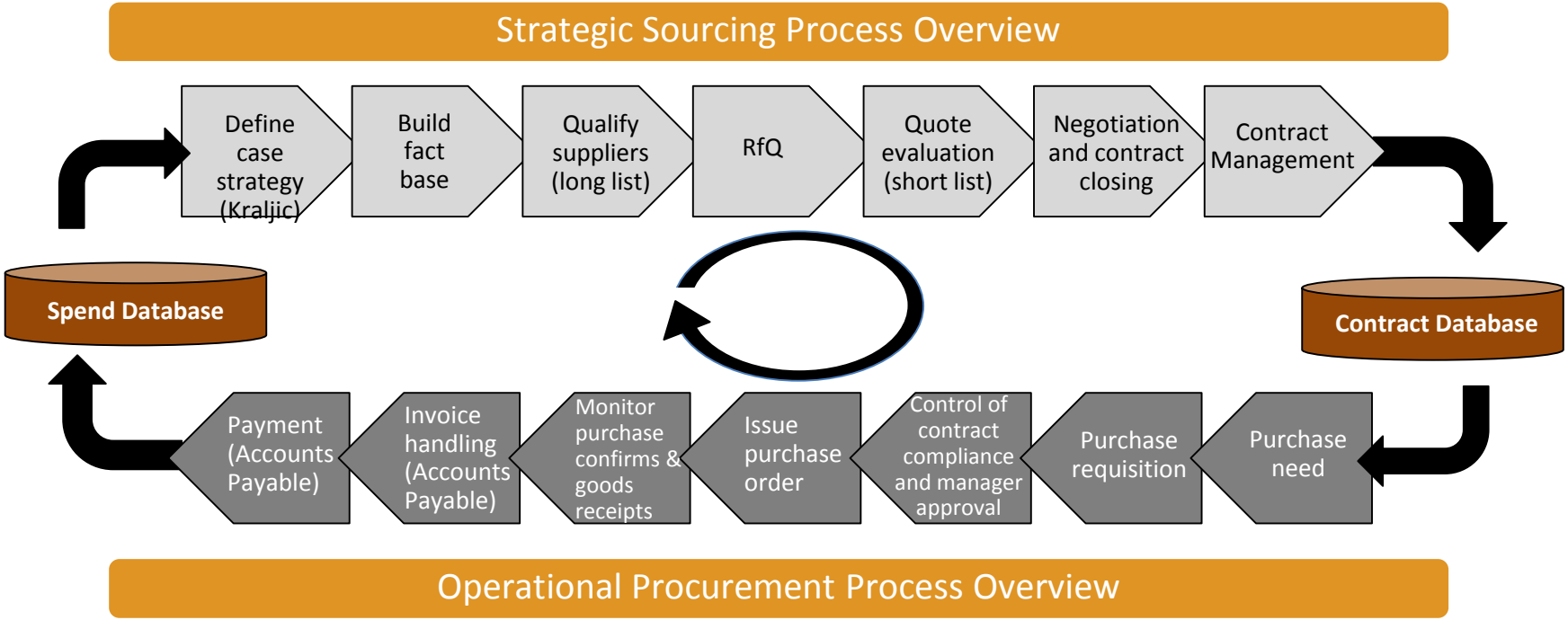
IT@UMN

THE SIGNIFICANT SECURITY INFORMATION CHALLENGE

- Our controls provide good due diligence to…
  - ✓ Reduce the frequency of security breaches
  - ✓ Minimize the impact of security breaches
- We have additional technical controls in place to protect our enterprise systems and high-risk data
- But, security incidents **will** occur
- The high-impact security breach **will** occur
- Security incidents from Experts will remain undetected… no matter the controls we implement

IT@UMN

Establishing a purchasing process



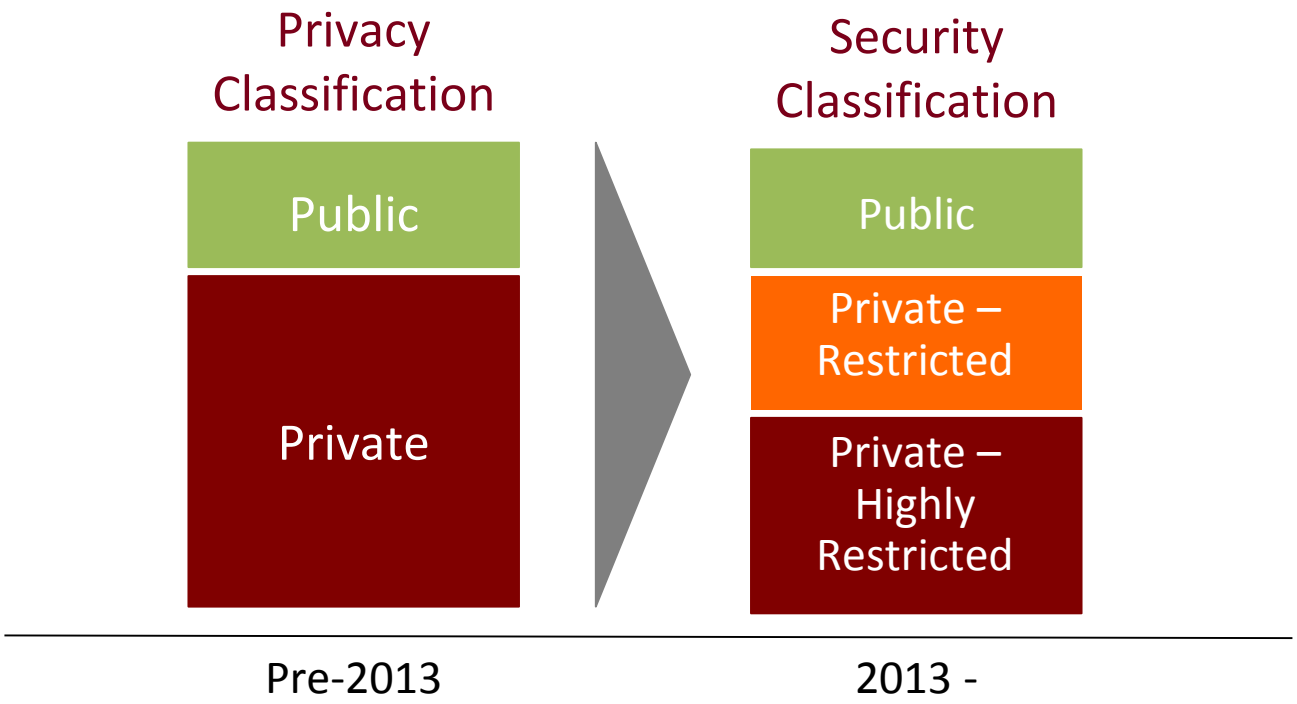
IT@UMN

Charge for University Information Security

- Create and manage an Information Security Program for the University of Minnesota system
- Establish and maintain an Information Security Framework that incorporates
  - ✓ Security Risk Management
  - ✓ Incident Management
  - ✓ Exception Management
- Maintain programs to assist meeting its regulatory requirements related to Information Security
  - ✓ Includes responsibility for HIPAA Security Officer

IT@UMN

DATA CLASSIFICATION

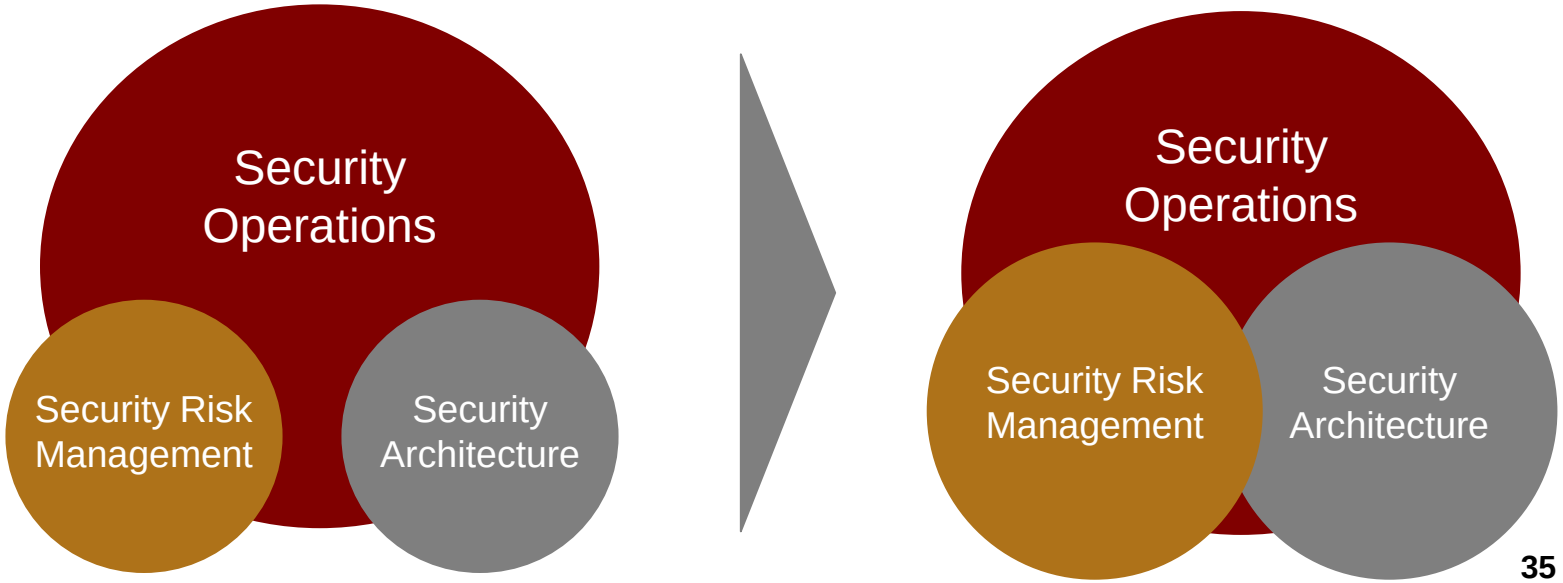


IT@UMN

University's Information Security Program Transition

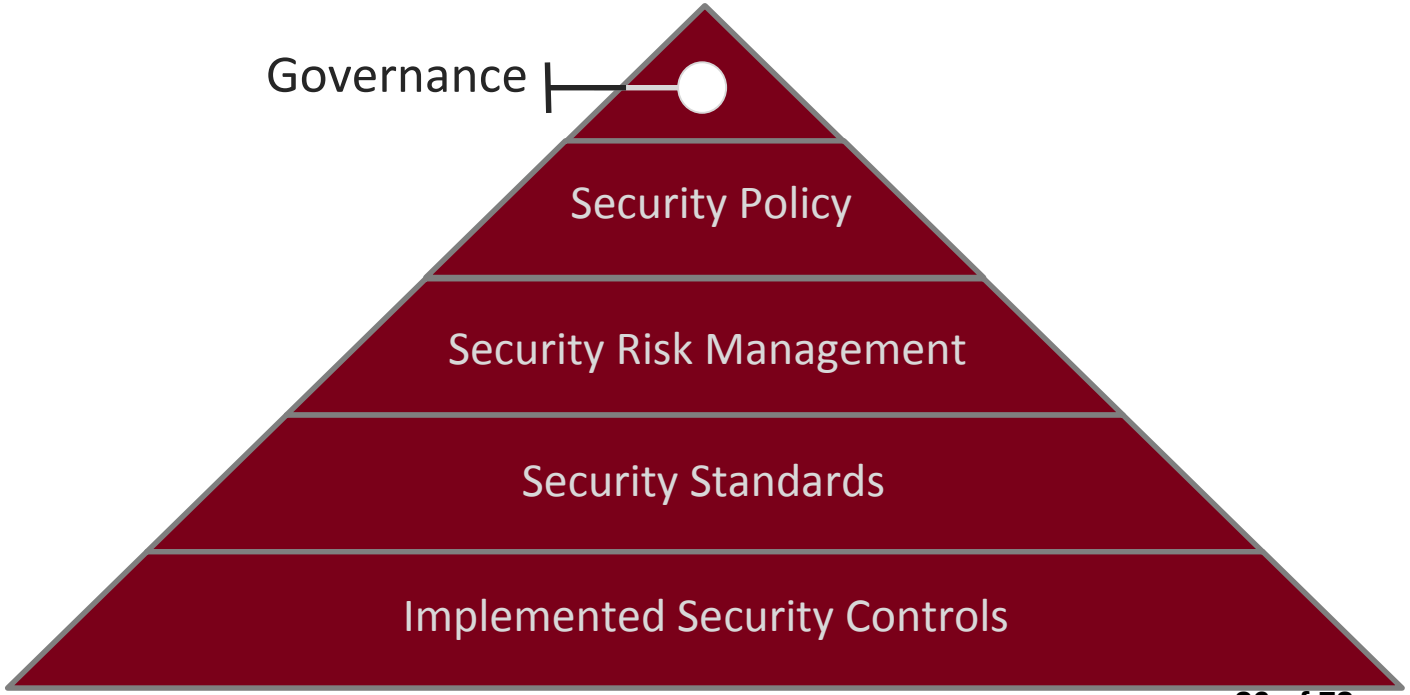
- Historic -
Reactive

- Future -
Proactively Manage Risk



IT@UMN

INFORMATION SECURITY FRAMEWORK MODEL



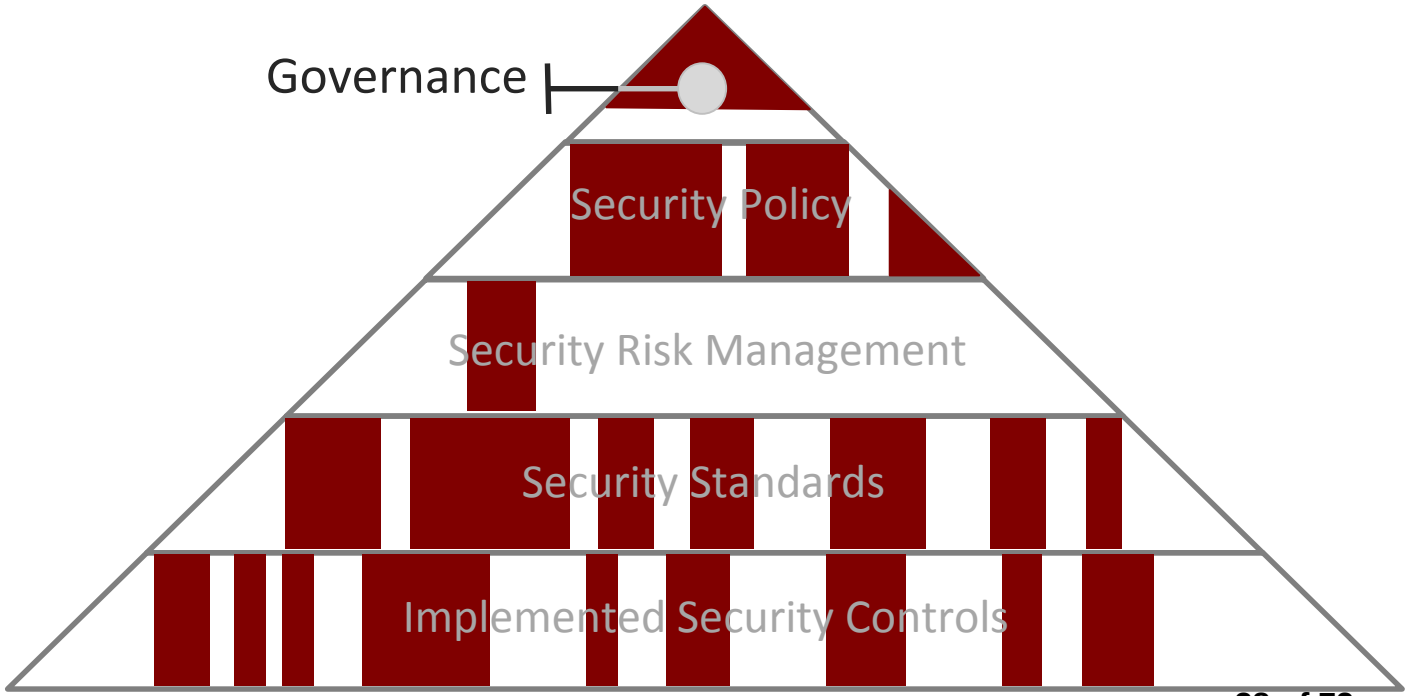
Security framework approach

Benefits

- Right security controls for the right risk level
- Focus on security controls with highest benefit
- Balance the benefit vs. the burden of the controls
- Reduce risk of regulatory compliance issues

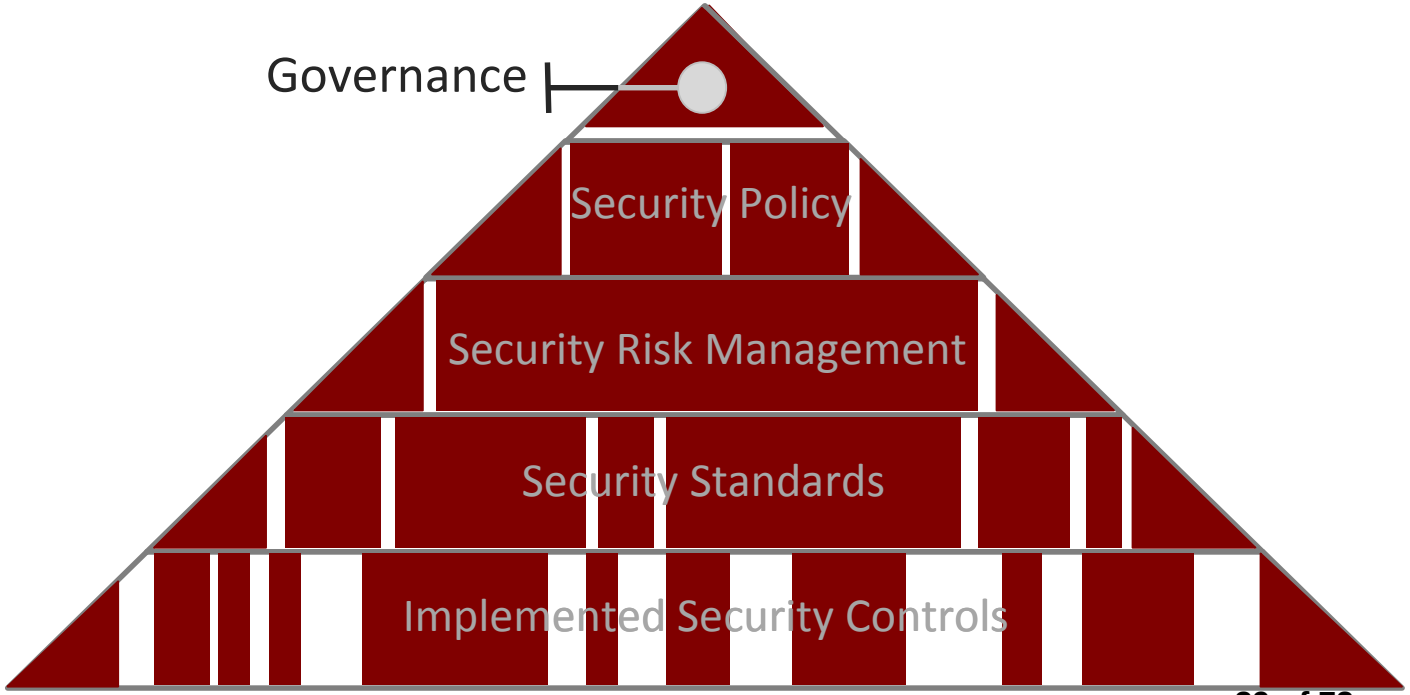
IT@UMN

University's information security framework – December 2010



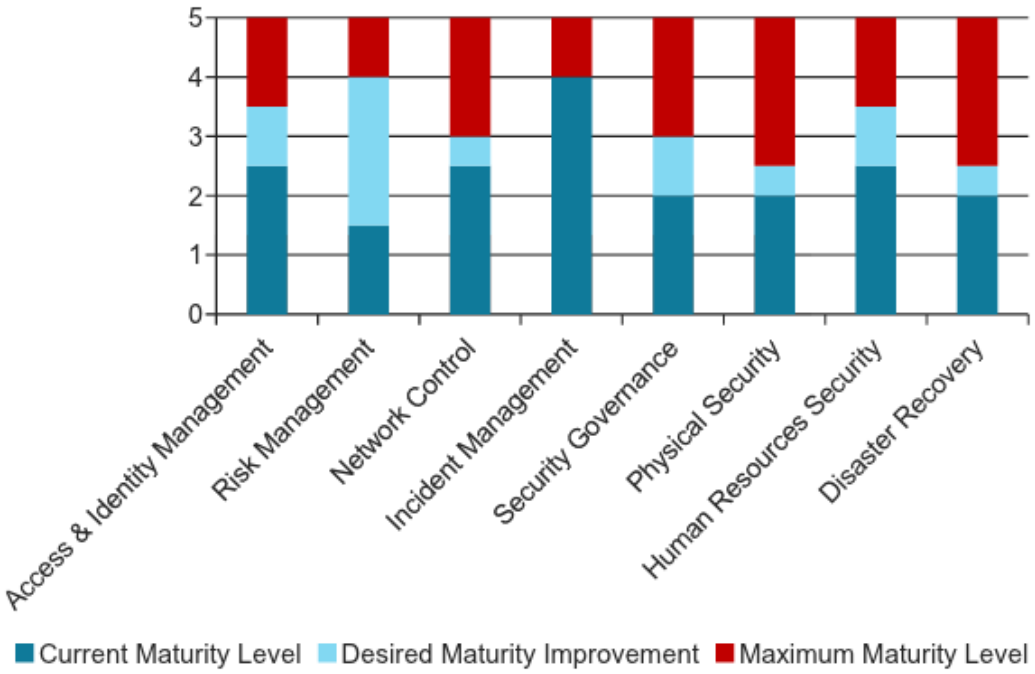
IT@UMN

University's Information Security Framework – December 2014



IT@UMN

INFORMATION SECURITY MATURITY ESTIMATE

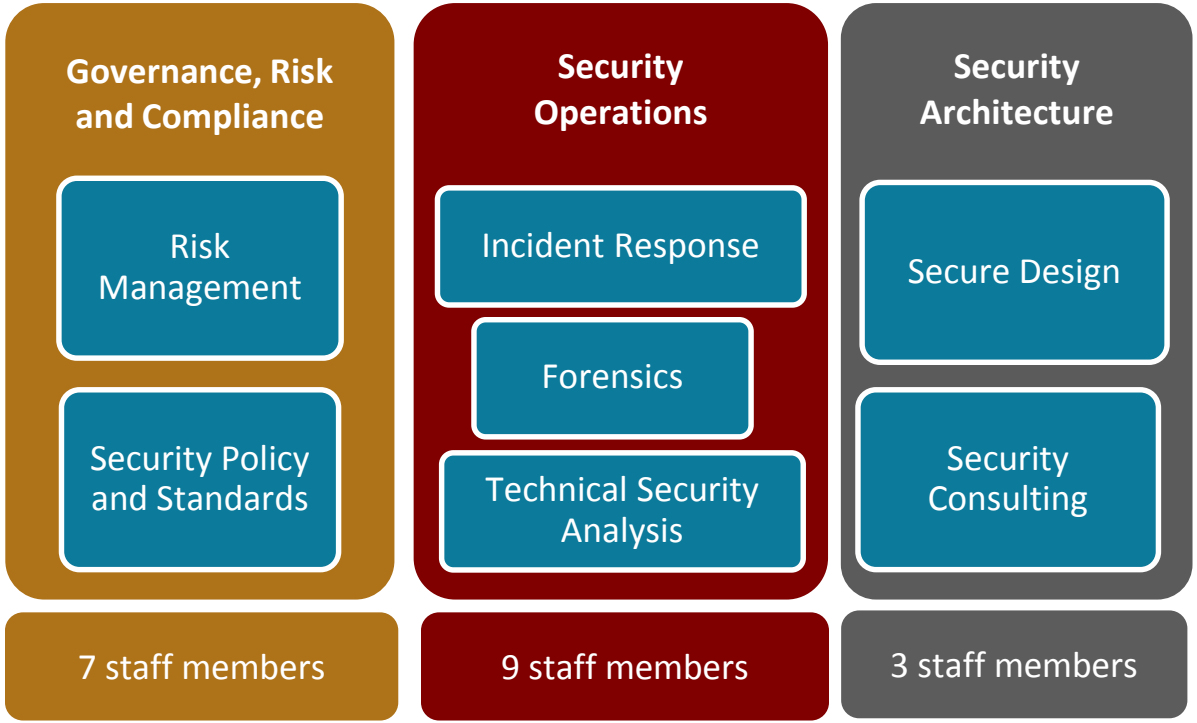


Notes

- Building from our maturity level will improve detection and prevention efforts for Errors, Amateur, Hobbyist threats
- Implementing controls to try to reach maximum security level results in:
  - Law of diminishing returns
  - Significant increased cost
  - Limited increase in security effectiveness
  - Significant impact to operational efficiency

IT@UMN

UNIVERSITY INFORMATION SECURITY TEAM

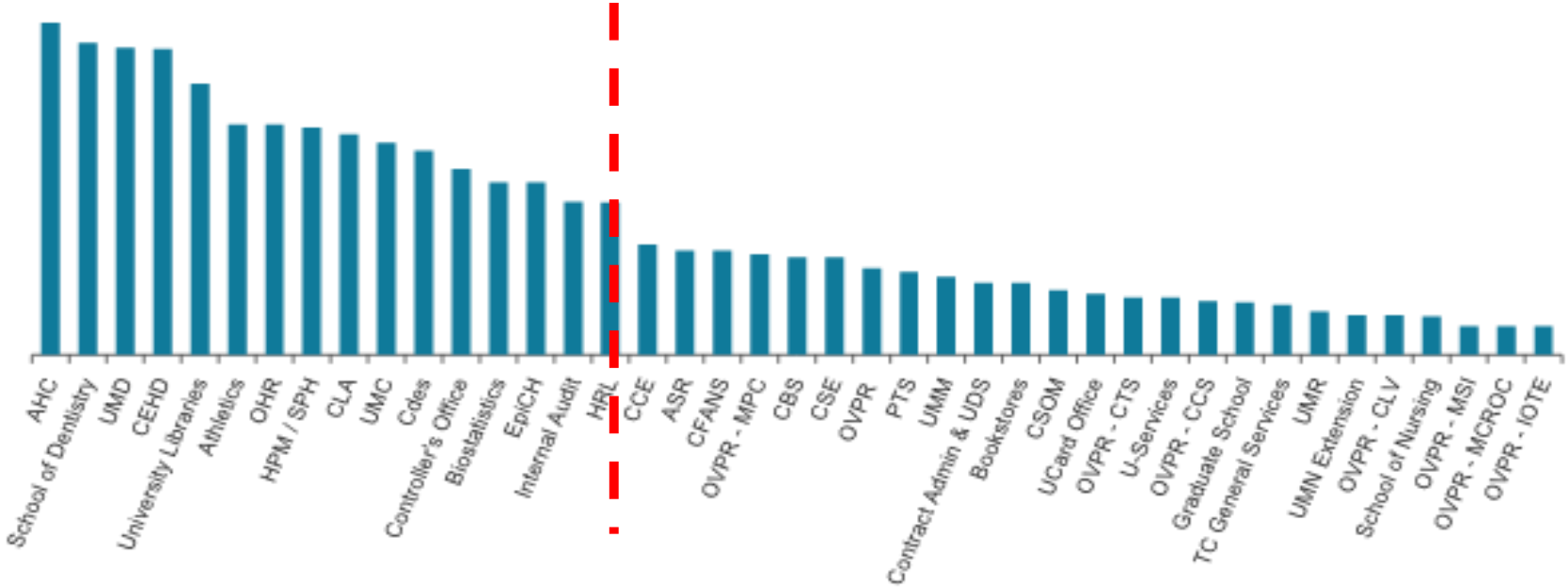


Information Security Staff:
19 members have 21 accreditations

- Certified Information Security Manager (1)
- Certified Information Systems Security Professional (5)
- Certified Information Systems Auditor
- Global Information Assurance Certification Forensic Analyst (2)
- Global Certified Intrusion Analyst
- GIAC Security Essentials Certification
- GIAC Certified Incident Handler
- GIAC Certified Web Application Penetration Tester

IT@UMN

PLANNED RISK ASSESSMENTS



IT@UMN

INFORMATION SECURITY STANDARDS

Before

Securing Private Data Policy

Basic

- Training
- Authentication
- Configuration
- Firewall
- Anti-Virus
- Security Patches

Enhanced

- Access Control
- Virus Protection
- Security Patches
- Local Data Owner
- Encryption
- Data Storage
- Physical Security
- Backups
- Technical Vulnerability Management
- Secure Data Deletion & Secure Disposal
- Change Control
- Log Management
- Risk Assessment

After

Information Security Policy

Security Levels: High, Medium and Low

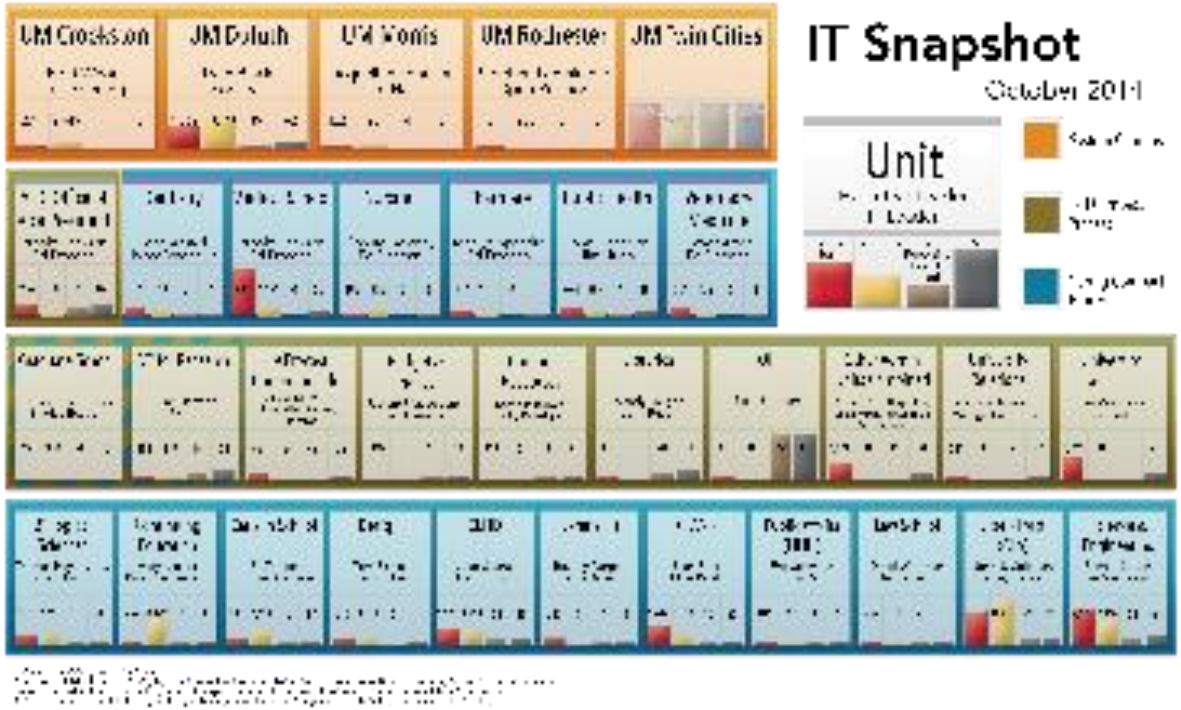
- Access Control - Application
- Access Control - Mobile
- Access Control - Network
- Access Control - OS
- Access Control - User Responsibilities
- Account Provisioning
- Backups
- Change Control
- Data Center Operations, Storage
- Encryption – End-User Device
- Firewall - Device, Network
- Information Security Awareness, Education and Training
- Management of End-User Device
- Media Sanitization
- Physical Security
- Risk Assessment
- Security Patches
- Strong Authentication
- Technical Vulnerability Management - IT Professionals
- Technical Vulnerability Management - U Community
- User Administrative Privilege
- Virus/Malware Protection

PATCHING MULTI-YEAR SYSTEMS (E.G., SERVER, PRINT SERVER)

Process	Security Level	Security Level	Security Level	
	High	**Medium**	**Low**	**Requirement**
Monitor for security-related patches for the operating system and applications	Required	Required	Recommended	Current
Apply security patches within 30 days of release from the vendor	Required	Required	Required	Current
Use operating systems and applications where the vendor or active open source community develop current security patches	Required	Required	Required	Current
Remove previous versions of applications if the patching process does not automatically remove older versions	Required	Recommended	At your discretion	New
Document a process for managing the security patches for the operating system and applications	Required	Recommended	At your discretion	New

IT@UMN

Distributed nature of information technology



IT@UMN

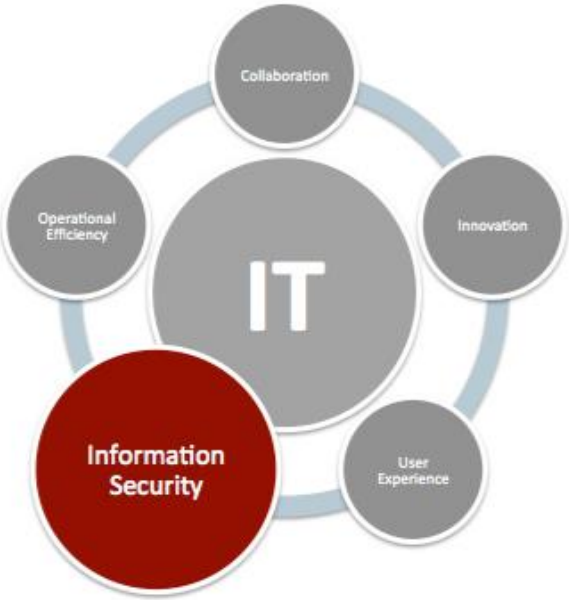
Confidence in strategy and focus

- High level of confidence with strategy… managing natural tension within open culture of higher education
- University is expanding scope of Security Advisory Committee to review and guide efforts
- Modeling program on principles in internationally accepted security framework (ISO 27001/27002)
- In contact with other Big Ten institutions, FBI, others to share information on security threats and protocols
- Accessing industry best practices to be prepared

IT@UMN

Progress continues and more is expected

- Distributed nature of IT makes execution of Information Security program a challenge
- University and IT communities have been highly involved in development of program
- Formal “community of practice” up and running
- Brian’s experience, leadership and team are making an impact: among the leaders in Big Ten
- It’s a “marathon not a sprint” - We are aggressively focused on being planful and prepared



IT@UMN

THANK YOU!

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **December 11, 2014**

Agenda Item: Institutional Compliance Officer Semi-Annual Report

☐ **Review** ☐ **Review + Action** ☐ **Action** ☒ **Discussion**

☒ *This is a report required by Board policy.*

Presenters: Lynn Zentner, Director, Office of Institutional Compliance

Purpose & Key Points

This presentation provides the Audit Committee with information on the significant compliance matters that have arisen since the Compliance Director's last report. The presentation will help the committee carry out its oversight responsibilities of the University Compliance Program.

The report addresses the following:

- Ensuring safety on all University campuses.
- The importance of risk assessments.
- Working toward full compliance with the Payment Card Industry Data Security Standards.
- Conflict of interest disclosures nationally and at the University.
- Revised federal agency policies may create new compliance challenges.
- Clinical trials under review.
- Compliance related training/education.
- UReport statistics for calendar year 2014.

Background Information

Under Board of Regents Policy: *Audit Committee Charter*, the Audit Committee is responsible for the oversight of the institutional compliance program. The director last reported to the committee on February 13, 2014.

REPORT OF THE DIRECTOR, OFFICE OF INSTITUTIONAL COMPLIANCE, FOR THE AUDIT COMMITTEE OF THE BOARD OF REGENTS ON THE UNIVERSITY COMPLIANCE PROGRAM DECEMBER 11, 2014

INTRODUCTION

This report addresses the following: (1) Ensuring Safety on University Campuses; (2) The Importance of Risk Assessments; (3) Working Toward Full Compliance With the Payment Card Industry Data Security Standards; (4) Conflict of Interest Disclosures Nationally and At the University; (5) Revised Federal Agency Policies May Create New Compliance Challenges; (6) Clinical Trials Under Review; (7) Compliance Related Training/Education; and (8) UReport Statistics For Calendar Year 2014.

Additional information regarding the University's Office of Institutional Compliance is available on the Office's website. Links to relevant resources are also provided. http://www.compliance.umn.edu/complianceHome.htm.

I. ENSURING SAFETY ON UNIVERSITY CAMPUSES

During the reporting period, efforts undertaken by faculty and staff reflect the University's commitment to workplace safety.

A. EXPLOSION IN LABORATORY AT SMITH HALL

An explosion occurred in the Chemistry Department on the fourth floor of Smith Hall on June 17, 2014. A doctoral student was injured as a result of that explosion. His injuries were not serious; however, he was hospitalized for two days.

The chemical involved in the explosion was TMS azide ("TMS"), a chemical compound used as a reagent in organic chemistry. Although the amount of TMS used for the experiment conducted by the student was not determined to be substantially more than what is described in the experimental literature for the experiment, to avoid a repeat of the high energy explosion that occurred, the Chair of the Chemistry Department has since substantially limited the amount that can be used in a given experiment. The Department is also taking steps to ensure that potential energies of reactions are considered when determining if a reaction should be conducted.

The student had conducted the same experiment 12 times before the June 17 incident without incident. At the time of the explosion, the student was not wearing protective equipment as he was getting ready to leave the lab when he noticed something unusual about the chemical reaction, walked over to inspect the mixture, at which point the explosion took place. Although it may be difficult to identify exactly what caused the explosion, it is likely that it resulted from the introduction of moisture into the synthesis, overheating the mixture, or a combination of these factors.

The Chemistry Department Chair and others in the College of Science and Engineering had been extremely proactive on lab safety issues before the explosion occurred. Their efforts included unannounced visits to labs, rigorous safety training, and ongoing communications among PIs,

students, and department chairs. In fact, on the day of the explosion, lab safety training was taking place in the building where the explosion occurred. Ensuring the consistent use of personal protective equipment has also been addressed and will be managed even more closely in the future.

At the time the explosion occurred, the student was replicating an experiment/process described in professional journals. The Chemistry Department informed several publications about the incident including: Chemical and Engineering News, Bioorganic and Medicinal Chemistry Letters, Organic Synthesis (primary source), and Synthesis.

Following the explosion, the Office of Occupational Health and Safety was contacted by OSHA. Since the injured student is not a University employee, OSHA has no jurisdiction over this matter.

The Department of Environmental Health and Safety took the lead on the investigation partnering with the Department of Chemistry to identify root causes and preventive actions.

This was not an incident that could have been anticipated. Nonetheless, its occurrence underscores the importance of lab safety education and commitment to safe practices.

B. VIOLENCE AGAINST WOMEN ACT

The Office of Institutional Compliance has reported in the past on the additional requirements imposed by the revisions to this federal law which was signed into law in March 2013. Going forward, the Office of Equal Opportunity and Affirmative Action will investigate all sexual assaults alleged by students and staff, partnering with UMPD as appropriate, and with the Office for Student Conduct and Academic Integrity when students are involved.

Revised Federal regulations were issued on October 20, 2014. They become effective on July 1, 2015. The regulations provide further clarity for the revised statutory provisions that went into effect in March 2013. A few of the noteworthy provisions are described below:

- Revised the categories of bias for the purpose of Clery Act reporting to include gender identity and to separate ethnicity and national origin into separate categories;
- Require institutions to provide to incoming students and new employees and describe in their annual security reports information regarding prevention and awareness programs;
- Require institutions to describe the range of protective measures they may offer following an allegation of dating violence, domestic violence, sexual assault, or stalking;
- Require institutions to describe each type of disciplinary proceeding used by the institution; the steps, anticipated timelines, and decision-making process for each type of disciplinary proceeding, how to file a complaint, and how the institution determines which type of proceeding to use based on the circumstances of an allegation of dating violence, domestic violence, sexual assault, or stalking.

The University's policy*: Sexual Assault, Stalking, and Relationship Violence* was updated in January 2014 to comply with the changes resulting from revised Federal law. The Office of Equal Opportunity and Affirmative Action has responsibility for compliance with and implementation of the recent statutory and regulatory revisions. A major focus is and will continue to be on educating supervisors and faculty advisors regarding the requirements of the law and regulations and the processes the University currently has in place to ensure compliance.

In addition, University Services through the University's Police Department, has and will continue to have significant responsibility for Clery Act reporting. The Clery Act requires colleges and universities across the United States to publicly disclose information about crime on and around their campuses and to report certain statistics to the Department of Education.

Recent presentations have been given on the revisions to this law at a meeting of the Board of Regents Academic and Student Affairs Committee in September and at a meeting of the Operational Excellence Leadership Group in November.

II. THE IMPORTANCE OF RISK ASSESSMENTS

Three separate but related initiatives either have been or are currently underway to evaluate and manage risk in the context of information security.

A. ADMINISTRATIVE POLICY TITLED "INFORMATION SECURITY RISK MANAGEMENT"

An administrative policy, initiated by the Office of Information Technology (OIT) and adopted by the University in January of this year, requires the development of an annual security risk assessment plan in consultation with collegiate and administrative units. These units are responsible for cooperating with the implementation of the annual plan and, upon request, collaborating with the University's Chief Information Security Officer to complete security risk assessments and develop remediation plans if needed. The rationale for the policy is that it is critical that the University administer formal information security risk management processes in order to facilitate compliance with applicable state and federal laws and regulations, protect the confidentiality and integrity of University of Minnesota data, and enable informed decisions regarding risk tolerance and acceptance. Once risk assessments have been completed and risk areas identified and evaluated, OIT, in collaboration with individual colleges and administrative units, will determine how to most effectively manage identified risks.

B. HIPAA SECURITY RISK ASSESSMENT

HIPAA regulations require the conduct of risk assessments. The Office for Civil Rights (OCR) within the Department of Health and Human Services, considers a risk analysis to be the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the HIPAA Security Rule. According to OCR, the elements of a risk assessment should include:

- Defining the Scope of the Analysis;
- Data Collection (identifying where e-PHI is stored, received, maintained or transmitted);
- Identifying Potential Threats and Vulnerabilities;
- Assessing Current Security Measures Used to Safeguard e-PHI;
- Determining the Likelihood of Threat Occurrence;
- Determining the Potential Impact of a Threat Occurrence;
- Determining the Level of Risk;
- Documenting the Risk Analysis; and
- Conducting Periodic Reviews and Updates to the Risk Assessment.

The HIPAA Security Rule does not dictate or prescribe the frequency with which risk assessments are conducted but it is implied that they be ongoing. The circumstances of each environment will determine whether they are done annually, bi-annually, every three years, etc.

The University issued an RFP in May for the purpose of selecting a vendor to conduct a comprehensive HIPAA security risk assessment. Deloitte was selected. The risk assessment process began in early November and will likely continue through the end of this calendar year.

C. EXTERNAL INFORMATION SECURITY ASSESSMENT

In August, the Office of the Vice President of Information Technology/Chief Information Officer (OVPCIO) issued an RFP for an information security assessment intended to provide a strategic external assessment of the University's information security program strategy, planned implementation, and current maturity. In initiating this review, OVPCIO sought the expertise of a vendor to assist in establishing a quantifiable way of measuring where the University is today and where the institution should be. The selected vendor would also be responsible for providing the following:

- A baseline evaluation of the University's current information security program and recommendations regarding appropriate aspirational goals relative to other institutions of higher education;
- A written action plan that prioritizes proposed areas of focus;
- A proposed time frame for implementing key action items;
- Separate findings and recommendations regarding program strategy and operational implementation; and
- A final report that merges findings and recommendations into program strategies and operational implementation approaches.

Berry Dunn was selected as the vendor. The external review process began in September and an onsite visit occurred in October. The results of this review will inform strategic information risk tolerance discussions planned with the President's Operational Excellence Committee in December and the Audit Committee of the Board of Regents in May 2015.

III. *WORKING TOWARD FULL COMPLIANCE WITH THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS*

We have reported in the past on the application of the Payment Card Industry Data Security Standards (PCI DSS) that address security issues in the context of credit card transactions. These standards address the credit card process from the point of entry of credit card data into a system of records, to the processing of the data through the payment process. For example, credit cards are used for purchases made at the University of Minnesota Bookstores and for parking in University ramps.

An on-site assessment of the University's PCI DSS compliance was conducted by a Qualified Security Assessor (QSA) in January 2014. The QSA completed a report on compliance identifying areas in which the merchants and the University were not in compliance with PCI DSS. The report showed significant improvement over the assessment completed the previous year. The findings addressed in the report have been presented to individual merchants who are working through the remediation process. The QSA will return to complete another assessment

in January 2015. This assessment will be completed using version 3.0 of the PCI DSS (released in November 2013).

In an audit of Parking and Transportation Services (PTS) conducted by the Office of Internal Audit (report issued June 2014) it was noted that one system used by PTS did not meet PCI DSS requirements. Remediation of the issues identified is being handled by PTS in consultation with the QSA, the Controller's Office, and University Information Security (UIS). The QSA will review PTS systems again when conducting the University-wide on-site assessment in January 2015. In addition to the review that will be conducted by the QSA, UIS, in conjunction with the security risk assessment process it initiated in fall of 2014, will review units with PCI DSS data for information security risk in February 2015.

IV. CONFLICT OF INTEREST DISCLOSURES NATIONALLY AND AT THE UNIVERSITY

A. THE SUNSHINE ACT AND OPEN PAYMENTS WEBSITE

The Physicians Payments Sunshine Act ("the Sunshine Act") was enacted by Congress as part of the Patient Protection and Affordable Care Act. The Sunshine Act was signed into law in March 2010. The accompanying regulations went into effect in February 2013. The Act requires manufacturers of drugs and medical devices to report to the Secretary of Health and Human Services payments and transfers of value paid to teaching hospitals and physicians. The term "physician" includes dentists.

For several months during 2014, device and pharmaceutical companies reported to the Centers for Medicare and Medicaid Services (CMS) financial relationships those companies had with "physicians" during the last five months of 2013. Specifically, the companies reported payments made and other remuneration provided to physicians and dentists during the five-month timeframe to include consulting fees, honoraria, gifts, entertainment, food, travel subsidy, education support, research support, royalties, ownership or investment interests, compensation for serving as faculty or as a speaker for medical educational programs, and grants.

This information became publicly available on the Open Payments Database ("the database") on September 30, 2014. Conflict of Interest Program Staff ("program staff") identified all University physicians and dentists whose names appeared in the database and compared what the companies had reported to the information reported on the REPAs filed by these individuals for calendar years 2013 and 2014. As a result of this review, program staff identified discrepancies associated with 33 individuals. An inquiry was sent to each of the individuals for whom a discrepancy was found to determine if any had unmanaged conflicts of interest. All of the 33 matters have been resolved. This inquiry resulted in the recent development of conflict management plans for two individuals.

B. *REPA AND FDUO REPORTING AT THE UNIVERSITY*

As of October 31, the University achieved 100 % reporting with respect to both REPA (Report of External Professional Activities) and FDUO (Financial Disclosure of University Officials)

filing. There are currently 181 active conflict management plans in place. Of the 181 plans, 173 involve individual conflicts of interest and eight involve institutional conflicts.

V. UNIFORM GUIDANCE - REVISED FEDERAL AGENCY POLICIES MAY CREATE NEW COMPLIANCE CHALLENGES

On December 26, 2013, the Office of Management and Budget (OMB) issued regulations intended to streamline Federal government guidance on the requirements, cost principles, and audit requirements for federal research awards. Described as a "larger Federal effort to more effectively focus Federal resources on improving performance and outcomes while ensuring the financial integrity of taxpayer dollars in partnership with non-Federal stakeholders," this guidance is intended to provide a government-wide framework for grants management and, at the same time, "strengthen program outcomes through innovative and effective use of grant-making models, performance metrics, and evaluation." The new regulations are also intended to reduce administrative burden as well as the risk of fraud, waste, and abuse. The new regulations become effective on December 26, 2014. The guidance is not intended to broaden the scope of existing government requirements that govern Federal research awards to non-Federal entities. Despite these assurances, institutions of higher education, to include the University of Minnesota, are carefully assessing what the changes might be and their impact on the way that Federal grants are currently managed.

Staff in the Office of the Vice President for Research (OVPR) have developed a very helpful website, convened an executive committee and several work groups, and given presentations to numerous groups including the Council of Research Associate Deans, the Senate Research Committee, Certified Approvers, the Grants Management User Network, the Clinical Neuroscience Center, and at the February Sponsored Projects Symposium. In addition, OVPR staff submitted a letter to the National Science Foundation (NSF) in July endorsing a letter previously submitted to the agency by the Council on Governmental Relations and providing additional recommendations focused on adding clarity and avoiding additional burden in the federal research awards process.

VI. CLINICAL TRIALS UNDER REVIEW

A. BY THE ASSOCIATION FOR THE ACCREDITATION OF HUMAN RESEARCH PROTECTION PROGRAMS (AAHRPP)

In June of this year, in response to a resolution passed by the Minnesota Faculty Senate calling for an inquiry to examine current University policies, practices, and oversight of clinical research on human subjects, the University retained AAHRPP to logistically manage the inquiry process. By its resolution, the Faculty Senate seeks an examination of the current processes associated with clinical research involving adult participants with diminished functional abilities. AAHRPP is an independent, non-profit accrediting body that is internationally recognized as an organization that sets the highest quality and ethical standards for the protection of human subjects in research programs. AAHRPP retained a team of external, independent experts to conduct the inquiry. That inquiry began in the fall of this year and is continuing.

B. BY THE LEGISLATIVE AUDITOR

Also in June of this year, James Nobels, Minnesota's Legislative Auditor, agreed to conduct a preliminary review of the University's management of the CAFÉ drug trial which was underway from April 22, 2002 through August 8, 2005. Dan Markingson, an enrolled subject in that trial, committed suicide in May 2004 and, since then, questions have been raised about the conduct of that clinical trial. The review by Legislative Auditor Nobels continues.

VII. COMPLIANCE-RELATED TRAINING/EDUCATION

The Office of Information Technology and the Office of Institutional Compliance are coordinating efforts, under the direction of the Executive Oversight Compliance Committee, to devise a plan that would result in the creation of an inventory of all of the training that is currently occurring at the University. This inventory would identify, as to each training, whether it is compliance-related or whether it falls into some other category, whether the training is required, and if required, determine the frequency with which the training must be taken, and define the audience. The goals are to address administrative burden, determine what areas of risk require mandatory training and identify those that do not, eliminate training that is duplicative of other offerings, identify training that ought to be offered but currently is not, and identify approaches for more effective training.

VIII. UREPORT STATISTICS FOR CALENDAR YEAR 2014

UReport is the University's confidential web-based reporting service. This reporting service is provided by Navex Global, an independent company that provides similar services for hundreds of companies and universities. UReport is intended to be used to report violations of local, state and federal law as well as violations of University policy. This reporting system is not intended to be used for employment concerns that do not involve legal or policy violations or involve purely student concerns, or issues for which the University is not responsible. Reporters may submit reports either via a hotline or the web. Reports may also be submitted anonymously. Those who submit reports are expected to report good faith concerns and to be truthful and cooperative in the University's investigation of allegations.

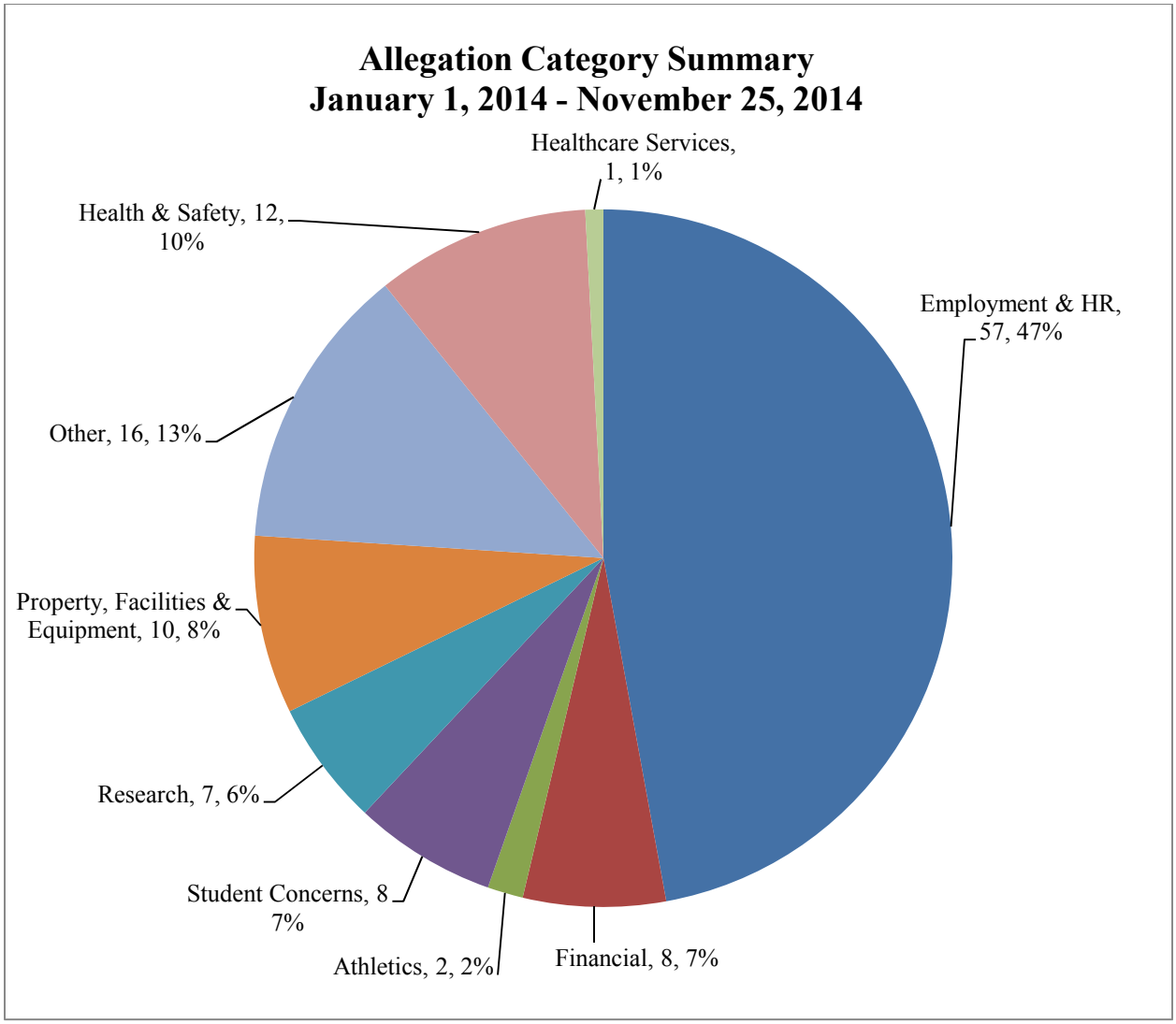
UReport has been in existence at the University since 2005. Since its inception, a total of 1201 reports have been submitted, averaging approximately 130 per year. During calendar year 2014 to date (1/1/2014 – 11/25/2014), 121 reports have been submitted; 89 reports were anonymous; and 90 reports involved allegations on the Twin Cities campus. Nearly 50% of the reports involve claims regarding:

- Hiring, advancement, discipline or termination
- Discrimination, harassment and/or equal opportunity
- Abuses in wage, benefits, vacation, overtime, and leaves
- Other employment concerns

Eighty-six percent of the reports are received via the internet. Sixty-two percent of anonymous reporters check back to determine the status of the follow up conducted regarding the concerns they have described. The graphs below illustrate these figures.

Issue		Running Total from Launch (August 2005)	January 1, 2014 to November 25, 2014
Total Reports		1201	121
Report Sources:			
	Internet	86%	86%
	Call Center	14%	14%
	Other	<1%	0%
% Anonymous		74%	73%
Reporter "check back rate" for anonymous reports		53%	62%

The following chart provides categorical breakdowns with respect to all allegations made in reports submitted in the previous 12 months.



BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **December 11, 2014**

Agenda Item: Information Items

☐ **Review** ☐ **Review + Action** ☐ **Action** ☒ **Discussion**

☒ *This is a report required by Board policy.*

Presenters: Gail Klatt, Associate Vice President

Purpose & Key Points

Office of Internal Audit Quality Assurance Self-Assessment Report

The Office of Internal Audit will be undergoing an external quality assurance review in February 2015. As part of the quality assurance process, the Office completes a self-assessment of its practices against the Institute of Internal Auditors' Standards for the Professional Practices of Internal Audit (Standards). The self-assessment, completed in November 2014, determined that the Office's practices are in conformance with the Standards. The review did identify selected areas where opportunities exist for continued improvement and plans have been developed for doing so.

Reporting of Engagements with Audit Firms

The Tweed Museum of Art entered into an engagement with Bradley P. Mickelson, CPA, to prepare a statement of financial activity as of June 30, 2014 to be used as financial support for grant applications. The fees for this engagement are not to exceed $1,900. This engagement did not impair the independence of Bradley P. Mickelson, CPA, as related to the University's external audit and was approved by the Controller's Office in conformance with Board policy.

The University of Minnesota Duluth entered into an agreement with Licari Larsen & Co., LTD to provide an audit of the financial statements of KUMD radio station as of June 30, 2014. This audit is being performed as a requirement for receiving grant funding from the Corporation for Public Broadcasting. The fees for this engagement are not to exceed $5,200. This engagement does not impair the independence of Licari Larsen & Co., LTD, as related to an external audit of the University and was approved by the Controller's Office in conformance with Board policy.

The University's Office of Student Affairs (OSA) seeks to engage the audit firm of Deloitte & Touche, LLP (Deloitte) to perform agreed-upon procedures for certain student groups receiving allocations of student fees from the University. Deloitte will perform the agreed-upon procedures on 23 student groups selected by OSA. The results of the procedures will evaluate the allocation of fees to student groups for FY 2014. The fees for this engagement are not to exceed $77,000. This engagement does not impair the independence of Deloitte & Touche, LLP

as related to an external audit of the University and was approved by the Controller's Office in conformance with Board policy.

Semi-Annual Controller's Report
The semi-annual Controller's Report provides information to the Board of Regents regarding recent activities in University financial operations which have strengthened financial reporting, enhanced internal controls, improved the management of financial risks, provided better services to the University community, and maximized the institution's financial resources. Highlights include:

- Analysis of new accounting standards that will be adopted by the University for FY 2015, and the likely impact to the University's annual audited financial reports (if known).
- Implementation of new federal Uniform Guidance requirements
- The status of the three year rollout of non-sponsored accounts receivable services and system tools to the University community.
- Information and considerations regarding non-audit engagements the University enters into with its external audit firm (currently Deloitte & Touche, LLP)

Background Information

The results of quality improvement and assurance processes are required to be communicated to the Audit Committee by the Office of Internal Audit's professional standards.

Engagements with audit firms are reported to the Audit Committee to assist the Regents in fulfilling their responsibility for oversight of engagements with external audit firms. Engagements with external auditors that do not require prior approval by the Board of Regents are reported after the fact to the Audit Committee as information items, in conformance with Board of Regents Policy: *Audit Committee Charter* and Board of Regents Policy: *Board Operations and Agenda Guidelines.*

The Controller's Report is prepared semi-annually and presented to the Audit Committee in conformance with Board of Regents Policy: *Board Operations and Agenda Guidelines.*

Quality Assessment
November 2014

EXECUTIVE SUMMARY

In accordance with The Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing (Standards)*, we conducted a quality self-assessment to ensure conformity with the *Standards*, evaluate the efficiency and effectiveness of the internal audit activity and identify opportunities for improvement. As part of the assessment, we evaluated the Office of Internal Audit's (OIA) ability to carry out its mission, including adding value and improving the operations of the University of Minnesota.

The self-assessment was performed using the methodology outlined in the IIA's 2013 *Quality Assessment Manual* and included compiling and reviewing detailed documentation, confidential staff surveys and surveys of senior leaders to obtain sufficient documentation to allow us to assess and support overall compliance with the *Standards*. We also reviewed the OIA's risk assessment and audit planning processes, audit tools and methodologies and engagement and staff management processes to assess the broad spectrum of OIA's activities.

We found the OIA to have a well organized structure conducive to compliance with the *Standards*. OIA has a well established rapport with senior leaders of the University and the Board of Regents, lending OIA the support and credibility needed to effect necessary change. The reporting relationship of OIA provides the independence and objectivity necessary to fulfill its responsibilities. The audit staff is highly capable with complementary and auxiliary expertise in information systems, research, investigations, and data analysis. We found the risk assessment methodology and processes to be particularly well developed and sound; the results, of which, are valued and leveraged for institutional purposes. The information systems planning, risk assessment and coverage is progressive, capitalizing on an effective partnership with the Office of Information Technology.

OPINION AS TO CONFORMITY TO THE STANDARDS

The IIA's Quality Assessment Manual suggests a scale of three ratings, "Generally Conforms," "Partially Conforms," and "Does Not Conform." "Generally Conforms" means that an internal audit activity has a charter, policies, and processes that are judged to be in conformance with the Standards. "Partially Conforms" means deficiencies in practice are noted that are judged to deviate from the Standards, but these deficiencies did not preclude the internal audit activity from performing its responsibilities in an acceptable manner. "Does Not Conform" means deficiencies in practice are judged to be so significant as to seriously impair or preclude the internal audit activity from performing adequately in all or in significant areas of its responsibilities. It is our opinion that the Office of Internal Audit *generally conforms* to all major standards in effect on the date of our review and *generally conforms* to most supporting standards (see exhibit A). A summary of partially conforming standards are as follows:

- 1220 – Due Professional Care
  The Office of Internal Audit does not currently have a formal and fully functional data analytics program. Queries and/or reports are run using Excel or the University's Data Warehouse as needed to support audit testing. Beginning January 2015 OIA will purchase and begin training to use a data analytic software called Arbutus.

Recommendation: OIA should carry out its plans to include data analytics more prominently in future audits through the use of Arbutus and increased training to advance the data analytics competencies of the staff.

- 2240 – Engagement Work Program
  For one of the four audits tested the IT audit programs were not found in the approved planning file. OIA's process is that IT audit programs are approved prior to the start of field work by a principal IT auditor that has been delegated the role of audit program approval.
  Recommendation: OIA needs to ensure all audit programs are approved, signed-off and included in the appropriate file in a timely manner, when hand-offs occur between work teams.

- 2340 – Engagement Supervision
  Some workpapers files for one of the four audits tested were not found to be formally approved. However there was evidence the files were reviewed.
  Recommendation: OIA needs to ensure that the approval of all workpapers is formally documented to evidence thorough and complete review.

Our review also identified some opportunities for improvement beyond the items above that were classified as partially conforming:

- The performance management system should be re-evaluated to determine the reason why more than a third of employees believe improvements could be made with the frequency, adequacy and helpfulness of performance reviews.
- The Office of Internal Audit does not have formal training requirements each year for staff members to fulfill. Staff members attend trainings to fulfill professional certification requirements or attend trainings they think are beneficial to their responsibilities; however, there is no minimum yearly credit requirements imposed by the OIA.
- OIA does not have a formal onboarding process to assist new staff members.
- The University finalized its strategic plan on 9-12-14. OIA can now begin to familiarize itself with the University's plan and tailor its audit work to align with its strategic objectives.
- OIA should formalize it's Quality Assurance and Improvement Program (QAIP) plan, and specifically communicate it results to the Audit Committee at least annually.

Appendix E1

Evaluation Summary: Quality Assessment

(GC = Generally Conforms, PC = Partially Conforms, DNC = Does Not Conform)

Quality Assessment Evaluation Summary—Overall Evaluation	GC	PC	DNC
OVERALL EVALUATION	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
1000	Purpose, Authority, and Responsibility	X		
1010	Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter	X		
1100	Independence and Objectivity	X		
1110	Organizational Independence	X		
1111	Direct Interaction with the Board	X		
1120	Individual Objectivity	X		
1130	Impairment to Independence or Objectivity	X		
1200	Proficiency and Due Professional Care	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
1210	Proficiency	X		
1220	Due Professional Care		X	
1230	Continuing Professional Development	X		
1300	Quality Assurance and Improvement Program	X		
1310	Requirements of the Quality Assurance and Improvement Program	X		
1311	Internal Assessments	X		
1312	External Assessments	X		
1320	Reporting on the Quality Assurance and Improvement Program	X		
1321	Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"	X		
1322	Disclosure of Nonconformance	X		
2000	Managing the Internal Audit Activity	X		
2010	Planning	X		
2020	Communication and Approval	X		
2030	Resource Management	X		
2040	Policies and Procedures	X		
2050	Coordination	X		
2060	Reporting to Senior Management and the Board	X		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
2100	Nature of Work	X		
2110	Governance	X		
2120	Risk Management	X		
2130	Control	X		
2200	Engagement Planning	X		
2201	Planning Considerations	X		
2210	Engagement Objectives	X		
2220	Engagement Scope	X		
2230	Engagement Resource Allocation	X		
2240	Engagement Work Program		X	
2300	Performing the Engagement	X		
2310	Identifying Information	X		
2320	Analysis and Evaluation	X		
2330	Documenting Information	X		
2340	Engagement Supervision		X	
2400	Communicating Results	X		
2410	Criteria for Communicating	X		
2420	Quality of Communications	X		
2421	Errors and Omissions	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
2430	Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"	X		
2431	Engagement Disclosure of Nonconformance	X		
2440	Disseminating Results	X		
2450	Overall Opinions	X		
2500	Monitoring Progress	X		
2600	Communicating the Acceptance of Risks	X		
	The IIA's Code of Ethics	X		

UNIVERSITY OF MINNESOTA
BOARD OF REGENTS AUDIT COMMITTEE
SEMI-ANNUAL CONTROLLER'S REPORT
December, 2014

This report presents a summary of activities completed by the Controller's Office in the last six months that have strengthened financial reporting, enhanced internal controls, improved the management of financial risks, provided better services to the University community, and maximized the institution's financial resources and financial operations.

I. Accounting and Financial Reporting Matters

The Governmental Accounting Standards Board (GASB) has issued a number of new accounting and reporting standards that will be effective for fiscal year 2015. The following provides a brief summary of each new standard, and where known, the likely impact.

- **GASB Statement No. 68**, *Accounting and Financial Reporting for Pensions—an amendment of GASB Statement No. 27*, which establishes and improves accounting and financial reporting for defined benefit and contribution pension plans administered through trusts or equivalent arrangements. This statement is effective for the fiscal year ending June 30, 2015.

  GASB 68 will apply to the University, and the impact to our financial statements is expected to be material. The University will be required to record a pro rata share of pension liabilities, pension expense, and deferred inflows for both the Minnesota State Retirement System and Public Employees Retirement Association pension plans. The State has not completed the actuarial studies of those pensions, so the dollar amount of the impact is not available at this time. (Note – all governmental entities in the state who participate in these plans will similarly be required to record pro rata liabilities and expenses for these plans).

- **GASB Statement No. 69,** *Government Combinations and Disposals of Government Operations,* was issued in January 2013. It establishes accounting and financial reporting standards related to combinations and disposals of government operations, such as mergers, acquisitions, and transfers of operations. This statement is effective for the fiscal year ending June 30, 2015. At this time, we believe GASB 69 will have no impact on the University's financial statements.

- In November 2013, the GASB issued **Statement No. 71**, *Pension Transition for Contributions Made Subsequent to the Measurement Date—an amendment of GASB Statement No. 68*, which addresses the accounting and financial reporting matter identified with the implementation of GASB 68. The provisions of this statement will apply to the University, and it will be applied simultaneously with the implementation of GASB 68 for the fiscal year ending June 30, 2015.

II. Activities to Enhance Service, Productivity, and Efficiency, and to Improve Internal Controls

Implementation of New Federal Uniform Guidance Requirements

On December 26, 2013 the federal Office of Management and Budget issued new guidelines for federal grants management through one "super" circular, entitled *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* ("Uniform Guidance", or "UG"). The Uniform Guidance is intended to standardize requirements across multiple federal circulars applicable to different types of recipients (hospitals, nonprofits, universities, etc); ease the administrative burden on recipients of federal funds; and reduce the risk of waste, fraud, and abuse. The majority of requirements in the UG become effective on December 26, 2014, while the effective dates for new provisions applicable to certain procurement activities have been deferred into calendar year 2015.

During the past year, a team of experts from across the University, including key personnel from the Controller's Office, has been meeting to analyze the requirements of the new Uniform Guidance and its implications for the University's current policies and procedures. Some of the areas that will be impacted include:

- Purchasing and vendor payments
- Federal funding that is received by an organization, and then passed through or awarded (via subcontract) to other organizations
- Allowability and treatment for various types of costs, such as travel or indirect costs
- Program income
- Necessary approvals and required certifications

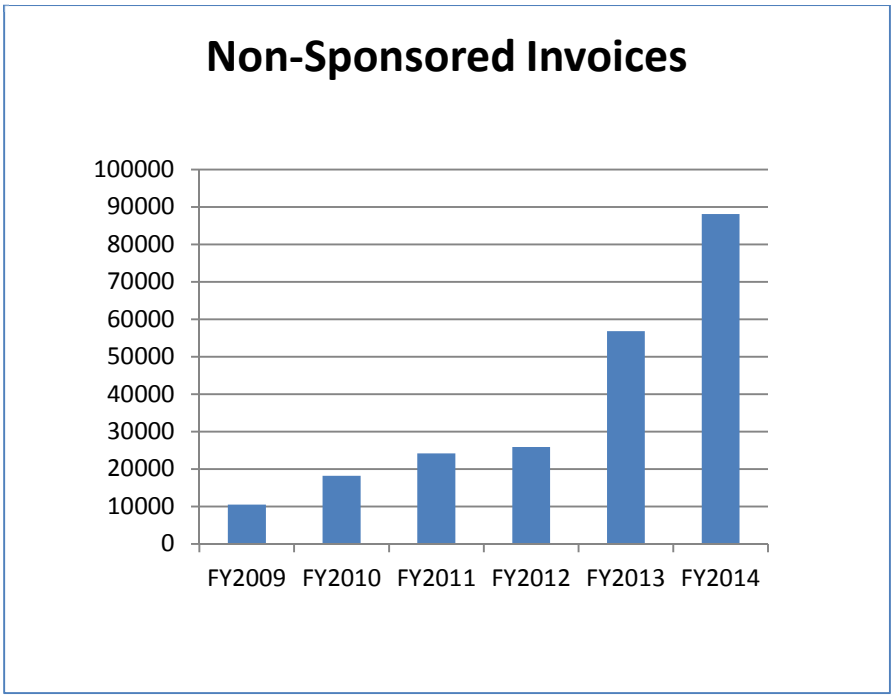
In December the University team will be providing options and recommendations for adjusting policies and procedures to University senior leadership. Implementation will begin in early 2015 to ensure that the University is prepared to receive and manage federal funds in compliance with requirements.

The UG requirements will apply to all new awards or additional funding to existing awards made on or after December 26, 2014. We are awaiting implementation plans from the various federal agencies, which will provide further guidance on the impact to existing federal awards received prior to December 26, 2014.

Roll-out of Non-sponsored Accounts Receivable services

In FY 2009 new financial management tools and practices were initiated for billing and cash collections on non-sponsored sales activity (i.e., excluding federal and state funding and tuition). The goals were to leverage the new PeopleSoft enterprise financial system's capabilities as a way to reduce the "shadow systems" across campus, improve the security over cash collections, and get more timely revenue information into the system, to improve the quality of financial information. Between FY 2009 and FY 2012, there was limited success in getting voluntary adoption of the new tools. So, at the beginning of FY2013 the Controller's Office began a three year project to complete the automation and centralization

of all invoicing and cash collections. During this time, departments have continued to convert billing activity to the Enterprise Financial System (EFS). The chart below shows the progress over the past six years.



At least 14 new departments have converted to EFS billing within the last 6-12 months:

- Office of Measurement Services
- UMD Recreational Sports Outdoor Program
- Continuing Education and Conference Center
- School of Music/Ted Mann Concert Hall
- Agronomy & Plant Genetics
- Plant Disease Clinic
- Water Resources Center
- Minnesota Agricultural Student Trainee program
- Minnesota Landscape Arboretum
- Caenorhabditis Genetics Center
- Natural Resources Research Institute
- Northrop
- Gopher Sports Spaces

Part of the three year project also included implementation of several system enhancements. One such feature is collections automation. The system automatically e-mails customers with past due items at pre-defined intervals. This feature has reduced the amount of time

spent sending collection correspondence, and notifies the customer of past due items more timely than manual processes.

Customers continue to utilize an online web application (introduced in 2011) to pay their invoices via credit/debit card. This fully automated payment method now accounts for 20% of the payments received for non-sponsored invoices and represents a very efficient means of receiving payment for invoices.

III. Non-audit Engagements with External Auditors

Background

In the past two years, there has been an increase in non-audit engagements between the University and Deloitte & Touche, LLP. As our official external audit firm, it is important that Deloitte protect and maintain its independence with respect to the audit work that it performs. The table below provides an overview of audit and non-audit fees paid to our external audit firms for calendar years 2010-2013, and the estimated or contracted amounts for engagements to date in calendar year 2014:

Calendar Year	Firm	Audit & Audit-Related Fees	Non-Audit Fees
2010	Larson Allen	$ 546,531	0
2011	Deloitte	$ 571,504	0
2012	Deloitte	$ 580,703	0
2013	Deloitte	$ 626,366	$ 1,887,581
2014	Deloitte	$ 606,800	$ 2,599,000

At the September 2014 Audit Committee meeting, the Audit Committee raised a question about whether the level of non-audit engagements awarded to Deloitte posed any independence issues. The Committee asked for information about applicable laws, regulations and best practices, the practices of other organizations, and other perspectives to help assess the question.

Auditor Independence

The primary concern when audit firms provide both audit and non-audit services is that the firm's "independence" will be impaired by the non-audit services. To evaluate this concern, it is useful to look at the laws and regulations dealing with auditor independence.

There are typically two components to auditor independence. The American Institute of Certified Public Accountants' (AICPA) definition of independence describes them as:

1. *Independence of mind*—the state of mind that permits the performance of an attest service without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

2. *Independence in appearance*—The avoidance of circumstances that would cause a reasonable and informed third party, having knowledge of all relevant information, including safeguards applied, to reasonably conclude that the integrity, objectivity, or professional skepticism of a firm or a member of the attest engagement team had been compromised. [1]

The Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board, and other federal and state regulatory bodies have also issued regulations and guidance to auditors about on the issue of auditor independence.

While the AICPA's definition is primarily aimed at accounting firms that are providing services to their clients, those clients, too, must understand and assess the risk that an audit firm may be performing work which is compromising the independence of the auditor. To that end, the SEC has published guidance for audit committees on auditor independence. Although it is directed at boards of publicly-traded companies, the guidance is nevertheless helpful for other entities in evaluating independence concerns when their audit firms perform both audit and non-audit services. The following excerpt is particularly useful:

The Commission's general standard of auditor independence is that an auditor's independence is impaired if the auditor is not, or a reasonable investor with knowledge of all the facts and circumstances would conclude that the auditor is not, capable of exercising objective and impartial judgment on all issues encompassed within the audit engagement. To determine whether an auditor is independent under this standard an audit committee needs to consider all of the relationships between the auditor and the company, the company's management and directors, not just those relationships related to reports filed with the Commission. The audit committee should consider whether a relationship with or service provided by an auditor:

(a) Creates a mutual or conflicting interest with their audit client;
(b) Places them in the position of auditing their own work;
(c) Results in their acting as management or an employee of the audit client; or
(d) Places them in a position of being an advocate for the audit client. [2]

<u>Others Organizations' Policies and Practices</u>
The Controller's Office was able to glean a sample of practices from a variety of entities or industries on the matter of auditor independence. Following is information related to proxy service companies, institutional investors, and higher education institutions. Although not exhaustive, the information shows tendencies but no clear direction in these organizations' policies or practices.

- Proxy service firms – A review of the guidance and recommendations issued by 3 proxy service firms indicated they generally recommend that non-audit fees should not exceed audit fees plus audit-related fees.

[1] AICPA Code of Conduct, Section ET100 – Independence, Integrity, and Objectivity.
[2] U.S. Securities and Exchange Commission, Office of the Chief Accountant - *Audit Committees and Auditor Independence*

- Practices by institutional investors with respect to their holdings – Large institutional investors have a significant voice in corporate governance. They cast votes on proposals to appoint audit firms for the companies they have invested in, and sometimes they take positions on the real or perceived independence of those audit firms. A review of the positions taken by 8 large public and private institutional investors reveals some diversity in their policies and practices towards non-audit fees:
    - 4 define non-audit fees as "excessive", if they exceed 30-50% of audit and audit-related fees;
    - 2 have articulated concerns about non-audit fees being "excessive" but do not define it; and
    - 2 make no reference in their investing policies to concerns about non-audit fees, or only call for management to fully disclose services and fees with audit firms.
- Other universities – An internet search review of the institutional policies of a handful of large public and private universities found no general trend in their policies related to non-audit fees. Institutions that do address non-audit services generally adhere to the definitions of prohibited services described by the AICPA and the SEC. Other than that list, institutions generally do not have formal policies limiting non-audit fees. Some, such as the University of Chicago and NYU, defer the decision on non-audit engagements to a senior financial executive of their institution. (Institutions searched include University of Michigan, Michigan State University, New York University, Northwestern University, The Ohio State University, Rutgers University, and the University of Chicago)

University of Minnesota Procedures and Management's Views

The University of Minnesota's current practices ensure that the services provided during a particular engagement by an external audit firm would result in an impairment of their independence. Each proposed engagement is assessed by the Controller's Office in relation to the profession's and the SEC's lists of prohibited services, to evaluate whether the scope and nature of work would result in the audit firm performing in the role of management, or making decisions which they might later need to also audit. Additionally, engagements of $100,000 or more are reviewed and approved by the Board of Regents, pursuant to Board Policy.

However, the University does not currently evaluate whether the total value of non-audit services would appear to constitute an impairment of the auditors' independence. While University management agrees that the dollar amount of non-audit services is certainly one element to assess in evaluating audit independence, we believe it should not be the only criterion used to determine if non-audit service fees create an independence issue. We agree with the guidance provided by the SEC that there are multiple factors, including the professional relationship between the auditor, the organization, and its audit committee members, which need to be included in the assessment.

Management further believes that there are other factors that ought to be considered, in evaluating whether a threshold for non-audit services should be established. The first is likelihood that the amount of non-audit fees in relation to the total revenues of an audit form, are material enough to cause the external auditors to sacrifice their professional judgment or independence to preserve those fees. The amount of fees paid in the last few years is clearly significant, but probably not material in relation to the total annual revenues for Deloitte & Touche.

A second is the risk that prohibiting an audit firm from bidding on non-audit services would limit the number of qualified vendors that potentially able and qualified to perform work the University cannot perform itself. For example, in the past two years Deloitte has clearly demonstrated, through a competitive procurement process, that it was the best firm to perform non-audit services in relation to the University's enterprise asset management project. Had they been eliminated from bidding because of a dollar limit on non-audit fees, the University would have been forced to either hire a new audit firm, or accept another less qualified vendor.

Finally, establishing a black and white threshold for the amount of non-audit services an audit firm can provide would pose some challenges for both the University and an audit firm. How would decisions be made about which non-audit engagements the firm bids on and which engagements do not get bid on? Would the University be able to eliminate a firm early in a year, in anticipation of "more important" work later in the year? Could the University and the firm even discuss this situation without engaging in unfair procurement practices? And how would situations where an engagement extension or multi-phased engagements be handled?

Conclusion

Management does not recommend establishing a dollar threshold as the sole determinant for assessing whether non-audit engagement fees compromise an auditor's independence. As illustrated above, assessing auditor independence in non-audit engagement situations is a subjective process involving the specific relevant facts and circumstances. Management believes a full evaluation of all factors related to a proposed audit engagement or relationship is important to making the best decision in any particular situation. Management would be happy to discuss alternatives for improving the information provided to the Audit Committee as part of the recommendations to approve on non-audit engagements.