Audit Committee

September 2014

September 11, 2014

8:00 a.m. - 9:30 a.m.

East Committee Room, McNamara Alumni Center

AUD - SEP 2014

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 11, 2014**

Agenda Item: 2014–15 Committee Work Plan

☐ **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 establish the committee work plan for the upcoming year. The work plan ensures that the Audit Committee receives the information necessary to carry out the governance and fiduciary responsibilities assigned to it in Board of Regents Policy: *Audit Committee Charter*, including the supervision of the external auditor and oversight of the internal audit program. The committee also has an obligation to be informed regarding the institution's compliance program. This year's proposed work plan includes a series of discussions to inform the committee about information security risks and the institution's strategy for their mitigation.

Background Information

Each standing committee of the Board of Regents establishes an annual work plan. The work plan is a means to assist the Committee in discharging its responsibilities under Board of Regents Policy: *Audit Committee Charter* and provides a structure to ensure the topics of highest priority receive the Committee's attention.

In addition to Board of Regents Policy: *Audit Committee Charter,* Board of Regents Policy: *Board Operations and Agenda Guidelines* defines the role of the Audit Committee as follows:

> The Audit Committee oversees the University's system of risk assessment and internal controls, audits, financial reporting practices, and the institutional compliance program. This committee also provides a direct channel of communication to the Board for the independent auditor and internal auditors.
>
> Specifically, this committee:
> - recommends the engagement and related fees of the independent auditor to perform the annual financial audit of the University and required federal compliance audits;
> - approves all engagements of external audit firms;

- annually reviews the results of the independent auditor's work;
- recommends appointment or removal of the director of audits;
- reviews the director of audits' annual audit plan and approves subsequent material revisions to the plan or the department's budget; and
- recommends changes in the Office of Internal Audit Charter.

This committee also reviews:

- the annual financial statements, prior to issuance;
- periodic Office of Internal Audit reports, including a report on the implementation of audit recommendations;
- semi-annual controller reports;
- the independent auditor's annual audit and management letter; and
- responses to questions regarding audit issues, reports on enterprise systems, administrative program reviews, and other items relevant to the audit function.

Audit Committee Work Plan
2014-2015

Items in bold are topics presented in addition to the required agenda items.

Date	Topics
2014	
September 11-12	• **Office of Internal Audit Charter (Fiduciary/Governance)** • **Information Security Risk Primer (Education)** • Internal Audit Update (Fiduciary) • 2014-2015 Committee Work Plan Discussion (Governance)
October 9-10	No Audit Committee • Even though the committee will not meet in October, it will need to review the annual financial statements prior to their finalization in mid-October. As in previous years, this will be handled by the Chair via a conference call. (Fiduciary) • **A work session will also be held to draft the institutional risk profile**
November	No BOR or Committee Meetings.
December 11-12	• **Institutional Risk Profile (Governance)** • External Auditor Report (Fiduciary) • **UMN Data Security Strategy (Fiduciary/Governance)** • Institutional Compliance Officer Semi-Annual Report (Governance) • Information Item: Semi- Annual Controller's Report (Fiduciary)
2015	
January	No BOR or Committee Meetings.
February 12-13	• External Auditor's Review of Completed Audit Work and Letter to Management (Fiduciary) • **OMB Uniform Guidance and its Impact on the University (Education)** • **Internal Audit Quality Assurance Review Report (Fiduciary/Governance)** • Internal Audit Update (Fiduciary)
March 26-27	No Committee Meetings.
April	No BOR or Committee Meetings.
May 7-8	• External Auditor Review (Fiduciary) • External Audit Plan (Fiduciary) • **External Assessment of UMN Data Security Program and Maturity (Fiduciary/Governance)** • Institutional Compliance Officer Semi- Annual Report (Governance) • Information Item: External Auditor Relationships and Services Provided (Fiduciary)
June 11-12	• Internal Audit Plan (Fiduciary/Governance) • Internal Audit Update (Fiduciary) • **Primer on HIPAA Compliance at the University (Fiduciary)** • Information Item: Semi-Annual Controller's Report (Fiduciary)
July	BOR Meeting and Retreat. Committees only meet if there are urgent items requiring action.
August	No BOR or Committee Meetings.

Other potential items

- Discussion with Robert Keuppers; previously served as Deputy CEO of Deloitte and was responsible for regulatory and professional matters in the United States. He currently is the Managing Partner for Deloitte LLP's Center for Corporate Governance.
- PCI Compliance for University credit card processing activities
- Overview of the Sunshine Act and the University's response

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 11, 2014**

Agenda Item: Information Security Risk Primer

☐ **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 first of three discussions around information security planned for FY15 to educate committee members about the University's approach to information security risk management and support the Board's fiduciary oversight of information technology (IT) security policies and programs.

Information security deals with the mitigation of risks from a range of adversaries. Amateur hackers motivated out of curiosity or a desire for personal fame operate at one end of a spectrum, while specialists and experts working on behalf of nation-states act out of national interest on the other. But the vast majority of security incidents relate to errors or mistakes by legitimate users, and a comprehensive information security program involves dedicating resources to identifying and preventing those types of incidents as well.

This primer will give an overview of the types of incidents encountered at the University and will analyze a sample of higher profile incidents at peer institutions and other well publicized examples. It will also categorize those incidents along the spectrum of adversaries and motivations so that incidents at the University can be understood in context. We will discuss how "risk" can be understood to be a function of both the skill of likely adversaries, as well as the value of the information we hold relative to other institutions of higher education, healthcare, and scientific research.

Future discussions 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 face, as well as provide an overview and assessment of the maturity of our policies and practices. Ultimately we seek to build a base of common understanding upon which committee members can discuss risk tolerance and provide guidance on the desired maturity level and financial and cultural cost/benefit tradeoffs inherent in investing in further maturing of our information security framework.

Potential discussion questions:

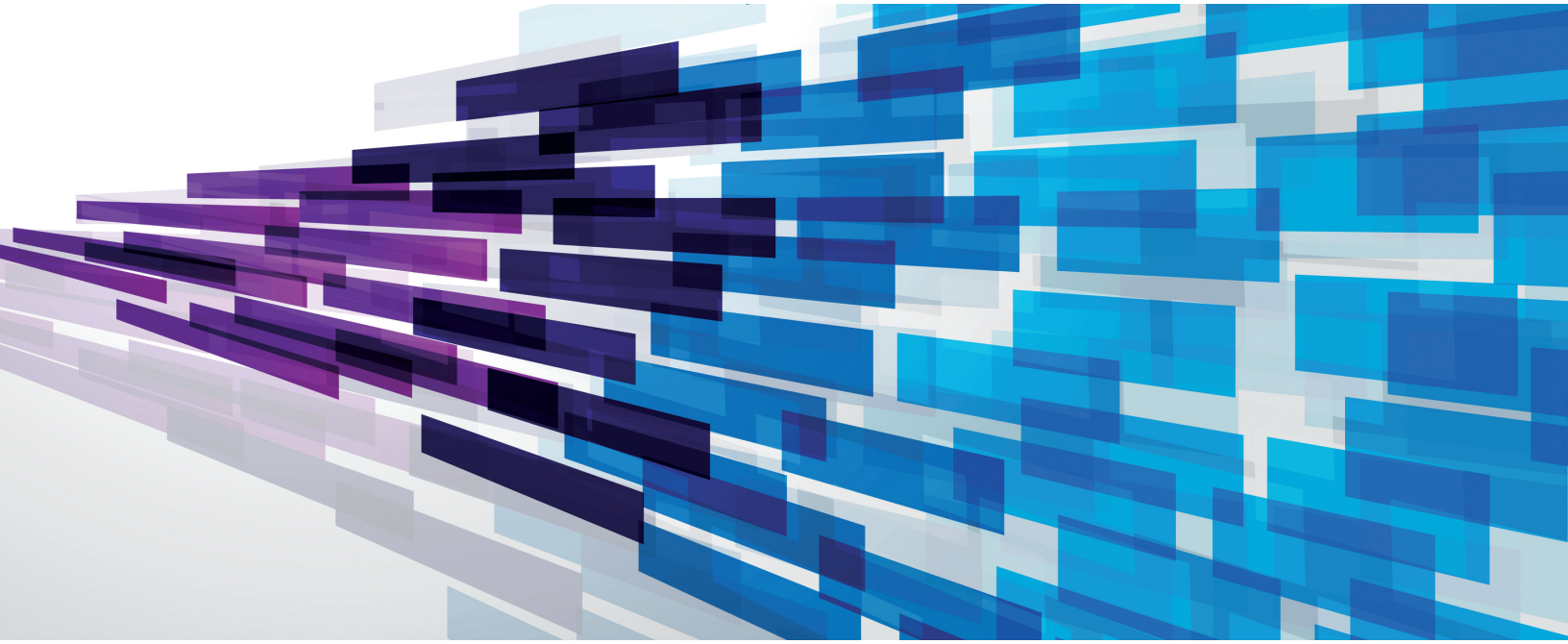
- Which types of incidents pose the greatest risk to the University, and what adversaries are likely to cause those incidents?
- How do we manage an information security program consistent with core values of academic freedom and openness?
- How do we establish and evolve policy at a pace consistent with emerging threats?

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-level 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.

CYBERSECURITY

WHAT THE BOARD OF DIRECTORS NEEDS TO ASK



The Institute of Internal Auditors Research Foundation

ISACA®
Trust in, and value from, information systems

Published by The Institute of Internal Auditors Research Foundation

247 Maitland Avenue

Altamonte Springs, Florida 32701-4201

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN-13: 978-0-89413-902-4

19 18 17 16 15 14 1 2 3 4 5 6 7 8 9

CONTENTS

ACKNOWLEDGMENTS

The project could not have been completed without the help of a team of professionals and subject matter experts.

Many thanks to the IIA and ISACA staff who dedicated many hours to project management, editorial, production, and marketing. A special note of recognition goes to the project review team:

The IIARF's Committee of Research and Education Advisors (CREA) volunteer members

Steve Mar, Team Lead

Steve Hunt

John McLaughlin

Mark Salamasick, former IIARF Board of Trustee member and Project Champion

Charles T. Saunders

Jason Thogmartin

David Williams

ISACA representative

Ron Hale, Acting CEO and Chief Knowledge Officer

ABOUT THE AUTHOR

With more than three decades of experience in IT, **Sajay Rai** brings a wealth of knowledge in information security and risk, IT audit, business continuity, disaster recovery, and privacy. Before starting Securely Yours LLC, Mr. Rai served as a partner of Ernst & Young LLP, responsible for the information advisory practice in the Detroit Metro area, and was also the national leader for Ernst & Young's security and risk practices. Prior to Ernst & Young, he was with IBM where he led their information security and business continuity practices.

He has served on The Institute of Internal Auditors' (IIA's) Professional Issues Committee (PIC) and as a board member of the Detroit Chapter. He has sat on the board of ISACA's Detroit Chapter and participated as a member of Walsh College's Accounting Advisory and Technology Committee. He holds a master's degree in information management from Washington University of St. Louis, and a bachelor's degree in computer science from Fontbonne College of St. Louis.

ABOUT THE RESEARCH SPONSORS

With more than 115,000 constituents in 180 countries, **ISACA** (www.isaca.org) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy, and governance professionals. ISACA offers the Cybersecurity Nexus, a comprehensive set of resources for cybersecurity professionals, and COBIT, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), and Certified in Risk and Information Systems Control (CRISC) credentials. The association has more than 200 chapters worldwide. ISACA has provided a cash contribution and donated time to The IIARF to produce this report.

The Institute of Internal Auditors Research Foundation (www.theiia.org/research) is a not-for-profit corporation whose mission is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally. Since 1976, The IIARF has been building a comprehensive, credible, and accessible repository of practitioner-reviewed content for the internal audit profession. The books and reports published by The IIARF provide forward-thinking research, current best practices, and insight into emerging issues. To support academic development of the internal audit profession, The IIARF also provides grants and awards for research by students and academic leaders. Finally, every few years The IIARF conducts the Global Internal Audit Common Body of Knowledge (CBOK), which is the world's largest survey of internal auditors (collecting approximately 13,500 responses from more than 107 countries). This data source is used for ongoing research and benchmarking.

INTRODUCTION

According to *Directors & Boards* author Tom Horton, "A primary responsibility of every board of directors is to secure the future of the organization. The very survival of the organization depends on the ability of the board and management not only to cope with future events but to anticipate the impact those events will have on both the company and the industry as a whole."

It is incumbent on the board of directors (board) to demand information and insight on the issues that could affect the future of the organization. Cybersecurity is one such issue. The overwhelming number of cybercrime incidents has forced boards to become more educated about the topic and ask strategic and thoughtful questions directed toward management and internal audit.

It is imperative that the board not relegate the cybersecurity topic to the IT department. Directors need to take an active role in the organization's cybersecurity or face the possibility of potential shareholder lawsuits, and even the possibility of being removed from the board.

The Institute of Internal Auditor's (IIA's) Audit Executive Center "Pulse of the Profession 2014"[1] survey reveals that boards are thinking about cybersecurity. When asked, "How would you characterize the board's perception of cybersecurity risks over the last one to two years?" more than 65% of respondents indicated that cybersecurity risks were at a high level or had increased. The table on the following page shows participant responses.

[1] Conducted between January 10, 2014, and February 2, 2014.

Response	Chart	Frequency	Count
Has been at a high level		8.5%	160
Increased significantly		18.7%	353
Increased		**40.8%**	**772**
Decreased		2.0%	38
Decreased significantly		1.1%	20
No change		28.9%	547
Not Answered			45
		Valid Responses	**1,890**
		Total Responses	**1,935**

On the other hand, when asked, "How involved was the board during the last fiscal year in regard to specific action or request on cybersecurity preparedness?" only 14% responded that they were actively involved in cybersecurity preparedness (see the responses in the table below). However, in the same survey, 58% of respondents said they should be actively involved in cybersecurity matters.

Response	Chart	Frequency	Count
Actively involved		14.1%	267
Involved		34.9%	662
Minimally involved		**36.1%**	**686**
Not sure of involvement		14.9%	283
Not Answered			37
		Valid Responses	**1,898**
		Total Responses	**1,935**

It is clear from this survey that the board would like to be strategically involved in the cybersecurity initiatives, but now the question becomes, "What should the board do?" The objective of this report is to provide recommendations on questions every board should ask and action items to take.

GUIDING PRINCIPLES FOR THE BOARD

The National Association of Corporate Directors (NACD), in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA), published a report outlining the five principles that all corporate boards should consider "as they seek to enhance their oversight of cyber risks."

The five principles[2] are:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Based on NACD's five principles, this report provides recommendations the board should consider implementing.

NACD Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

1. The board must assume the role of the fourth line of defense against cyber risks within the entire organization. In this capacity, the board must require internal audit to provide an annual "health check" report of the organization's cybersecurity program. This comprehensive report must cover all domains of the cybersecurity and be conducted by either the internal audit staff or an external security organization.

[2] *Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition* [National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA); Washington, DC; 2014]. Used by permission.

The board, as the fourth line of defense, must monitor whether the enterprise risk levels related to cybersecurity are improving or deteriorating from year to year. (See the appendix for further details on the lines of defense.)

> **Sarbanes-Oxley compliance provides little assurance of an effective security program to manage cyber threats.**

NACD Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

2. The board should understand the cyber risks associated with third-party service providers. With IT budgets shrinking and being asked to do more with fewer resources, outsourcing key components of IT or business processes to third-party service providers is becoming common.

Third-party service providers encompass a variety of services, but overall, the board should consider:

- IT outsourcing (e.g., data center, application development, help desk)
- Business process outsourcing (e.g., claims processing, payroll, engineering design, logistics, accounts payable, accounts receivable, background screening)
- Cloud solution (e.g., use of salesforce.com to perform key marketing and sales activity, use of box.net to share files and folders, Microsoft 365 to use cloud version of PowerPoint, Word, and Excel)

Most organizations are beginning to realize the potential security risks associated with third-party service providers. For instance, a potential risk is that an organization does not pay close attention to security and privacy when contracts are negotiated. Some third-party agreements do not clearly identify whether the service provider is responsible for safeguarding the organization's critical data or for notifying the organization in case of a data breach at the service provider's data center.

It is recommended that the board get a report of all the critical and vital business applications and the related data that is managed by third-party service providers. The board must make sure that the organization has appropriate agreements in place with the third-party provider and that the appropriate audit is performed regularly on the provider (e.g., SOC 1 and SOC 2 assurance reports).

In addition, the board should see that the organization has addressed the cyber risks associated with the concept of "chain of trust." The chain of trust requires that the third party have similar agreements with any downstream providers with which it has relationships.

3. Almost every state has enacted a data breach law that requires an organization to notify the state in case of a data breach, although the criteria of defining "what constitutes a data breach" may vary from state to state. From the board's perspective, the following information should be collected and understood:
   - In which states does the organization conduct business?
   - Are there states where the data breach and privacy laws may be stricter than others (e.g., Massachusetts and California are perceived to be "strict")?
   - What constitutes a data breach in those states?
   - What are the reporting requirements?
   - What safe harbor clauses are allowed under these state laws? For example, most of the state laws allow for an encryption safe harbor, which means that if the breached data is encrypted, reporting is not required or the reporting requirements are minimized significantly.

(For more details, refer to a detailed table of the laws by each state provided in Data Breach Charts by BakerHostetler LLP, a law firm based in Cleveland, Ohio. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.)

Outside the United States, most countries have passed or are in the process of passing privacy laws. If the organization is global, the board must take similar actions as identified above for those countries that have strict privacy laws and where the organization does business.

(For more details, refer to a document titled "2014 International Compendium of Data Privacy Laws" by BakerHostetler LLP. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.)

4. In light of several major data breaches around the world, it is recommended that the board is aware of all major data breach attempts made against the organization—not just the actual incidents but the major attempts as well. The definition of *major* may differ depending on the industry of the organization and whether the organization is global, national, or local.

> **Keeping track of attempted data breaches proves that an organization has an effective intrusion detection and incident response program.**

NACD Principle 3: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

5. Meet with the chief information security officer (CISO). Even though the board is getting the "health check" report from an independent source, it is recommended that the board take the time to meet with the CISO annually—at a minimum. The purpose of the meeting is to understand the state of cybersecurity within the organization and discuss key cybersecurity topics, including:
    a. Understanding key top-of-mind issues from the CISO's perspective
    b. Discussing the CISO's security strategy and current projects
    c. Providing the CISO with an opportunity to identify any key roadblocks (e.g., budget, political agendas, arrogance)
    d. Understanding the activities of data breaches within the organization's industry and how such knowledge is applied to the organization

> **The CISO is the "heart and soul" of an information security program in most organizations. There is no better way to obtain a pulse regarding cyber risk.**

6. Verify that management has established relationships with the appropriate national and local authorities who are responsible for cybersecurity or cyber-crime responses. For example, in the United States, verify that management has a relationship with the local Federal Bureau of Investigation (FBI), or better yet, meet with the FBI annually. The FBI has been actively involved in cybersecurity for more than a decade. In 1996, it formed a group called Infragard, a collaboration between the FBI and companies identified as being part of the nation's critical infrastructure.

The FBI is focused on a broad range of cyber threats from entities that are state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. The FBI is not only working in cooperation with federal, state, and local cyber task forces, but also with the National Cyber Investigative Joint Task Force (NCIJTF). It also coordinates overseas cybersecurity investigations and supports key partners, such as The Hague.

The FBI recently established a unit called Key Partnership Engagement Unit (KPEU), which manages a targeted outreach program focused on building relationships with senior executives of key private sector corporations. Through a tiered approach, the FBI is able to prioritize its efforts to better correlate potential national security threat levels with specific critical infrastructure sectors.

NACD Principle 4: Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

7. The board must require management to communicate the enterprise risk management organization structure and provide staffing and budget details. The enterprise risk management is generally comprised of several different risks, including but not limited to, operational, credit, regulatory, legal, and cybersecurity.

Management relies on different business groups to assist with enterprise risk management. For example, IT is a vital element of enterprise risk management and plays a key role in enabling the management of enterprise risks.

One of the budget data points the board must review is the total budget allocated to cybersecurity activity. It is recommended that the board review the following security budget metrics:

- What percentage of total revenue is the IT budget?
- What percentage of the IT budget is the security budget?
- How many security dollars are being spent per employee within the organization?
- Beyond corporate IT, what other departments maintain security budgets?

The board also must require management to provide statistics of how the industry allocates its budget to the above metrics.

> **The level of staffing and resources for the enterprise risk management program depend on the types of risks each organization has assessed. Depending on the industry to which an organization belongs, the budget percentages may vary. For example, regulated industries like finance and insurance allocate a higher percentage of the IT budget to security, whereas the manufacturing industry is typically at the low end.**

8. The board must ensure that the CISO is reporting at the appropriate levels within the organization. Keep in mind that, although many CISOs continue to report within the IT organization, sometimes the agenda of the chief information officer (CIO) is in conflict with that of the CISO. As such, the trend has been to migrate reporting lines to other officers, including the general counsel, the chief operating officer (COO), the chief risk officer (CRO), or even the chief executive officer (CEO), depending on the industry and the organization's dependency on technology.

> **In most organizations, the higher you are in the hierarchy of management, the more impact you can have on implementing policies and enabling culture change. Cybersecurity should be no different.**

NACD Principle 5: Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

9. Meet with the CRO or equivalent within the organization annually—at a minimum—and review all the risks that were either avoided or accepted.

There are times when a technology need is identified by a business unit and the business executive is convinced that it is the right solution for the organization. For example, the marketing and sales team hires a third-party vendor to host a solution for an upcoming marketing promotion. During a routine risk assessment performed by IT, potential security risks are identified and IT recommends that the solution is too risky for the organization and poses a potential risk of data exposure. In this case, the marketing executive decides that although the potential risks exist, he is willing to accept these risks and continue using the third-party vendor. He may even have the CEO's final approval.

In this example, the risk management process worked as designed. IT did its part and identified the risks. The business unit owner did his part by deciding to accept the risk (instead of agreeing with IT and searching for another solution). The business owner also followed the risk management process and notified the CEO of the decision.

In the research team's view, these types of risk management decisions can potentially open the organization to new or additional risks. But due to business pressures or other reasons, management accepts these risks and the board must be made aware of these decisions as part of the Risk Acceptance Report.

10. The board must verify that the cyber insurance coverage is sufficient to address the potential cyber risks. The board must ask management to provide the cost per record of data breach and understand the total potential impact of a major data breach.

> **A cybersecurity program is like an insurance policy. The expenditure on the cybersecurity program should not be more than the value of the assets it is protecting. Cyber insurance is a great complement to the entire cybersecurity program.**

SIX QUESTIONS THE BOARD SHOULD ASK

Having outlined the board's responsibilities regarding cybersecurity, there are also some questions it should consider that may help prepare for discussions with management and internal audit. For simplicity and brevity, each question outlines suggested action items.

1. Does the organization use a security framework?

   Action 1 ISO 27001 (The old British Standard BS 7799), NIST 800-53 (U.S. Federal Government comprehensive framework). COBIT framework (Governance, Risk, and Control)

   Action 2 HIPAA or HITRUST (for health-care industry)

   Action 3 PCI-DSS for credit card acceptance (retail industry, finance industry)

2. What are the top five risks the organization has related to cybersecurity?

The potential areas of risks are:

Action 4 Proliferation of BYOD and smart devices

Action 5 Cloud computing

Action 6 Outsourcing of critical business processes to a third party (and lack of controls around third-party services)

Action 7 Disaster recovery and business continuity

Action 8 Periodic access reviews

Action 9 Log reviews

Advanced persistent threats

3. How are employees made aware of their role related to cybersecurity?

The organization should have a security awareness training program, and each employee should be required to review the training and pass the test annually. The CEO (or other top executive) must communicate the importance of safeguarding the organization's critical assets.

4. Are external and internal threats considered when planning cybersecurity program activities?

Although external incidents tend to receive more media exposure, the likelihood of an internal incident causing a major cyber incident is actually greater than the external threat.

5. How is security governance managed within the organization?

Understanding the three lines of defense as they relate to the organization is important. There can be a gray area of security governance between the CISO and internal audit. It is important for the board to understand how the governance activities of the CISO complement those of internal audit.

6. In the event of a serious breach, has management developed a robust response protocol?

The potential areas are:

Action 10 Incident response program

Action 11 Crisis management program

Action 12 Crisis management team and their responsibilities

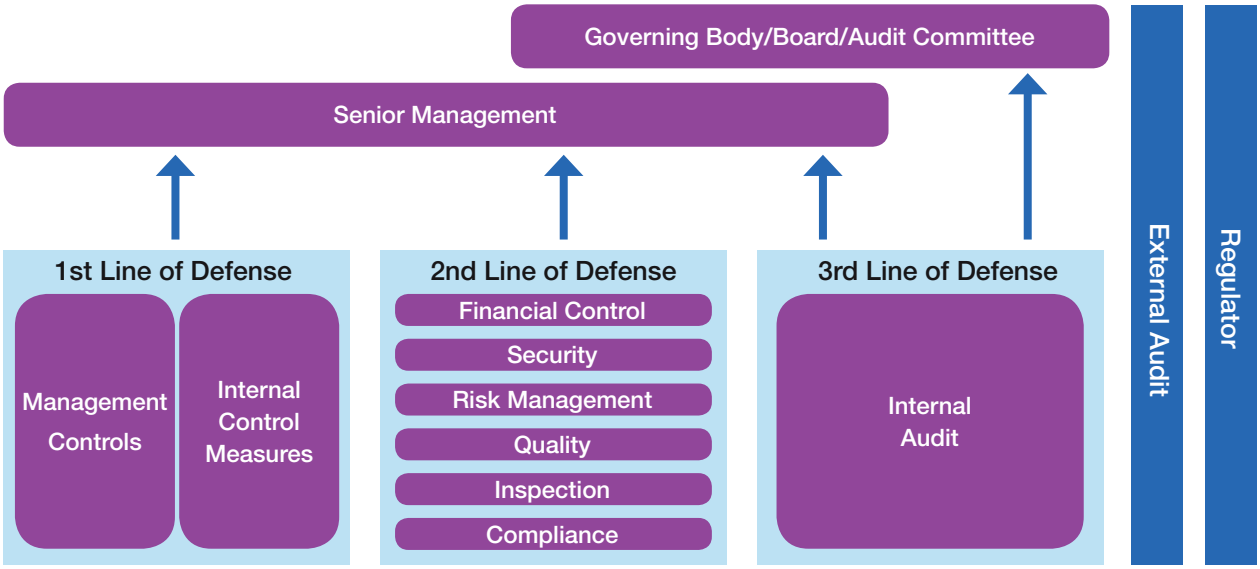
CONCLUSION

Cybersecurity will continue to pose a serious risk that the board needs to actively measure and continuously monitor as part of the organization's strategy. The questions and action items outlined in this report serve as a benchmark to guide the board, but the onus is on the board to take its strategic role seriously in providing oversight, implementing the plan, and becoming the fourth line of defense in cyber risk governance.

If the board is still not convinced, consider this: proxy adviser Institutional Shareholder Services (ISS) has urged shareholders to overhaul Target's board in the wake of last year's data breach. In a recent report, ISS recommended a vote against seven out of 10 directors "for failure to provide sufficient risk oversight" as members of the audit and corporate responsibility committees. Cybersecurity is no longer simply another agenda item for IT; it is an agenda item for the board as well.

APPENDIX

The three lines of defense concept helps organizations govern enterprise risks. The diagram below illustrates the concept of the three lines of defense.



If an organization has an effective governance model, the second line of defense is responsible for performing the majority of the governance functions related to cybersecurity. Typically, this role is headed by the CISO, who defines the policies, standards, and technical configuration standards.

The first line of defense (usually the IT operations function) then implements those policies and standards and is responsible for day-to-day monitoring of the networks and infrastructure. In its second line of defense, the CISO organization is responsible for governing those tasks and ensuring that IT is performing the appropriate monitoring, reporting, and tracking. As the third line of defense, internal audit is responsible for ensuring that the first and second lines of defense are functioning as designed.

REFERENCES

1. *Framework for Improving Critical Infrastructure Cybersecurity*. February 12, 2014. National Institute of Standards and Technology.
2. Audit Committee Leadership Network in North America. April 24, 2014. *ViewPoint*s, Issue 46.
3. National Exam Program, Risk Alert. April 15, 2014. Office of Inspection and Examination, Volume IV, Issue 2.
4. Audit Committee Leadership Network, Cybersecurity and the Board. 2012. *ViewPoints*. Waltham, MA: Tapestry Networks.
5. The Comprehensive National Cybersecurity Initiative. www.whitehouse.gov/isues/foreign-policy/cybersecurity/national-initiative.
6. Paez, Mauricio F., Richard J. Johnson, Steven G. Gersten, and Mina Saifi. February 20, 2014. U.S. Congress Ready to Enact Data Security and Breach Notification Rules After Recent Consumer Data Breaches, Jones Day.
7. Kelley, Matt. January 27, 2014. The Audit Committee Conundrum: IT Risks.
8. Kelley, Matt. February 18, 2014. Cyber-Security Takes Center Stage: Risks, Guidance, and Regulator Wrath. www.complianceweek.com/cyber-security-takes-centerstage-risk guidance.
9. Cybersecurity Legislation: Is Congress Ready? http://www.wiggin.com/14904.
10. Cybersecurity and Privacy. http://www.wiggin.com/12280.
11. http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml.
12. http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1.
13. http://blog.cybersecuritylaw.us/2014/04/16/the-fbis-role-in-cybersecurity/.
14. http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf.
15. National Cyber Security Strategies in the World. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.
16. http://www.corpgov.deloitte.com/site/us/audit-committee/risk-oversight/;jsessionid=VGTpTz1hLh26tykv5GNn2B0PJtCfxPpHLFfX2h1k51vl9n0n21dn!4557266!NONE.
17. Risk and Compliance Journal. deloitte.wsj.com/riskandcompliance/2014/05/28/embracing-digital-why-boards-that-don't-could-put-companies-at-at-risk/lab.
18. BakerHostetler LLP document on state-by-state privacy laws. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.
19. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

THE IIA RESEARCH FOUNDATION PARTNER RECOGNITION

The Mission of The IIA Research Foundation is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally. As a separate, tax-exempt organization, The Foundation depends on contributions from IIA chapters/institutes, individuals, and organizations. Thank you to the following donors:

STRATEGIC PARTNER

Crowe Horwath

PRINCIPAL PARTNERS

CaseWare Analytics
Deloitte & Touche LLP
Ernst & Young
Grant Thornton
PricewaterhouseCoopers
Thomson Reuters

DIAMOND PARTNERS (US $25,000+)

The Institute of Internal Auditors Chicago Chapter
The Institute of Internal Auditors Dallas Chapter

PLATINUM PARTNERS (US $15,000–$24,999)

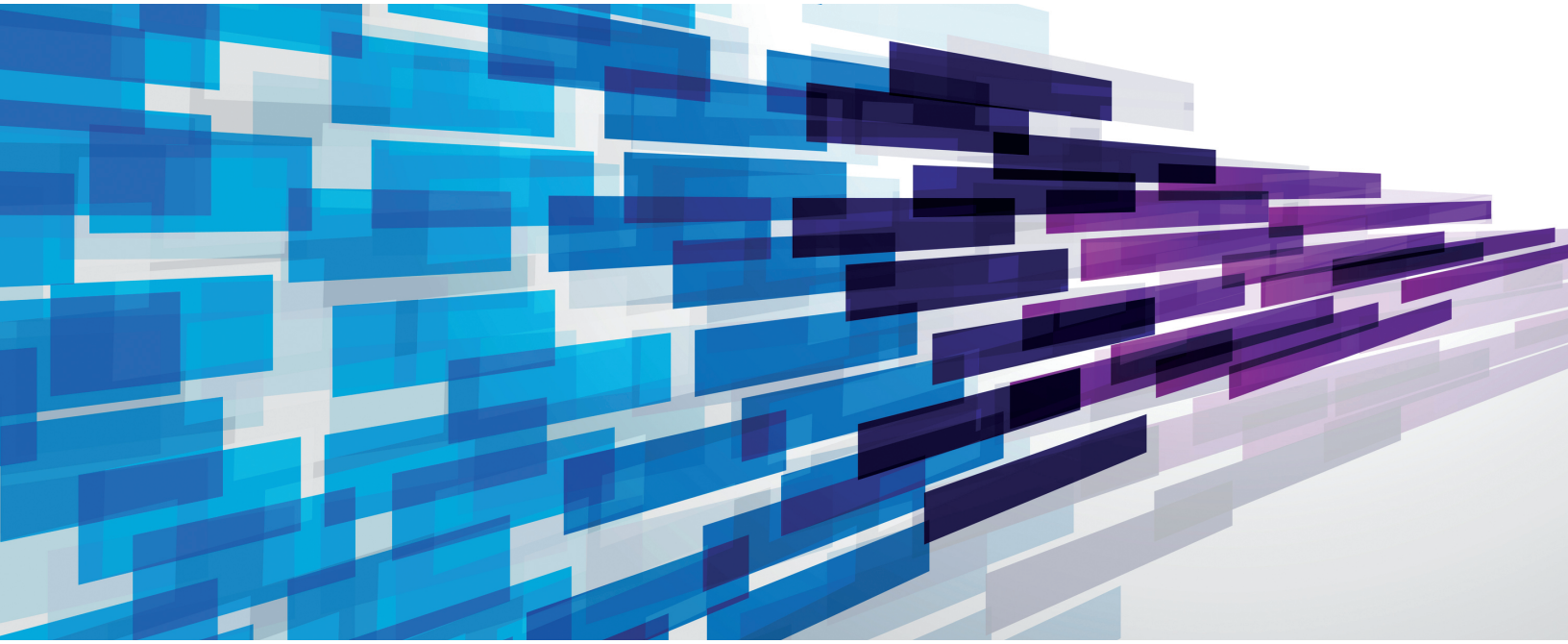
ACL
IIA–New York Chapter
IIA–Toronto Chapter

GOLD PARTNERS (US $5,000–$14,999)

Exxon Mobil
IIA–Austin Chapter
IIA–Detroit Chapter
IIA–Houston Chapter
IIA–Milwaukee Chapter
IIA–Philadelphia Chapter
IIA–Pittsburgh
ISACA

SILVER PARTNERS (US $1,000–$4,999)

Anthony J. Ridley, CIA
Bonnie L. Ulmer
Edward C. Pitts
IIA–Ak-Sar-Ben Chapter
IIA–Albany Chapter
IIA–Atlanta Chapter
IIA–Baltimore Chapter
IIA–Birmingham Chapter
IIA–Central Illinois Chapter
IIA–Indianapolis Chapter
IIA–Long Island Chapter
IIA–Miami Chapter
IIA–Nashville Chapter
IIA–Northeast Florida Chapter
IIA–Northern California East Bay Chapter
IIA–Northwest Metro Chicago Chapter
IIA–Sacramento Chapter
IIA–San Gabriel Chapter
IIA–San Jose Chapter
IIA–Southern New England Chapter
IIA–St. Louis Chapter
IIA–Tidewater Chapter
IIA–Tulsa Chapter
IIA–Twin Cities Chapter
IIA–Vancouver Chapter
IIA–Washington (DC) Chapter
Margaret P. Bastolla, CIA, CRMA
Michael J. Palmer, CIA
Paul J. Sobel, CIA, CRMA
Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
Stephen D. Goepfert, CIA, CRMA
Wayne G. Moore, CIA

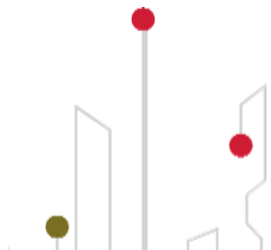


The Institute of Internal Auditors Research Foundation

INFORMATION TECHNOLOGY

Information Security

Scott Studham, Vice President for IT & CIO
Brian Dahlin, Chief Information Security Officer



UNIVERSITY OF MINNESOTA
Driven to Discover℠

IT@UMN

Information Security Presentations this Year with the Audit Subcommittee

September - Information Security Primer

- What Motivates the Hacker
- Awareness of Peer Institutions
- Review Recent Examples (Target, Higher Ed)

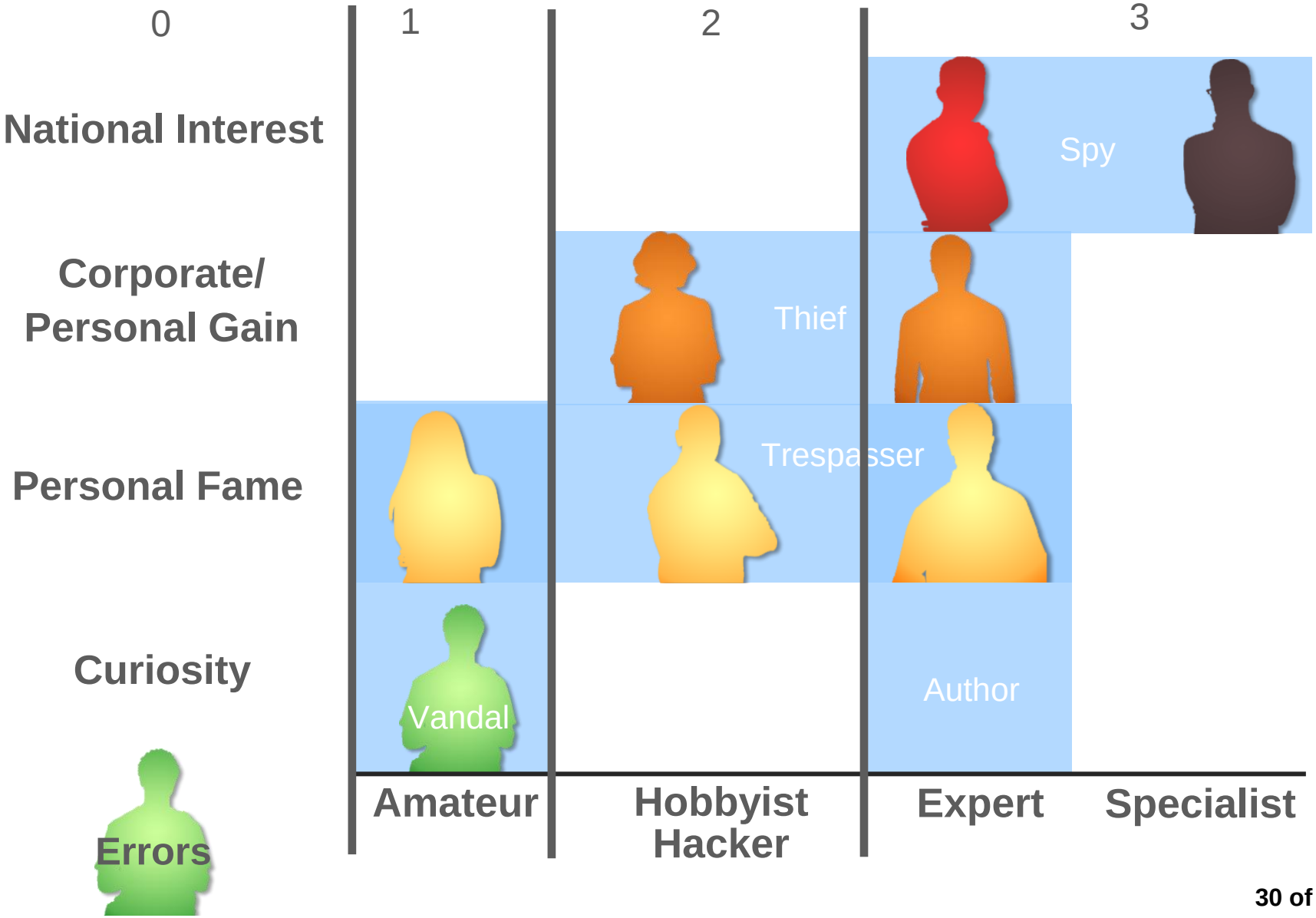
December - Information Security Program at UMN

- Overview of Information Security Program & Status
- Policy Standards & Risk Assessments

May - Risk Profile Discussion

- Debrief from Vendor on External Security Review
- Discussion about Recommendations

What Motivates an Adversary?



Never Underestimate the Motivation, Patience, and Creativity of an Adversary!

Adversaries:

- Play strength to weakness
- Develop surprising partners
- Have no rules
- See offense as a systems challenge
- Attack against a defense that is naïve, arrogant, unbalanced and fragmented

VOCABULARY

Security Incident – When the security of an information system, service, or network *could* have resulted in a breach of private data. An information security policy may have been violated or a safeguard may have failed.

Breach – The unauthorized acquisition, access, use, or disclosure of data maintained by the University, which compromises the security and privacy of the data.

Investigation - The process of collecting additional information on a security incident to determine if additional actions (such as whether a breach notification is required) are needed.

Record – The data set related to one individual.

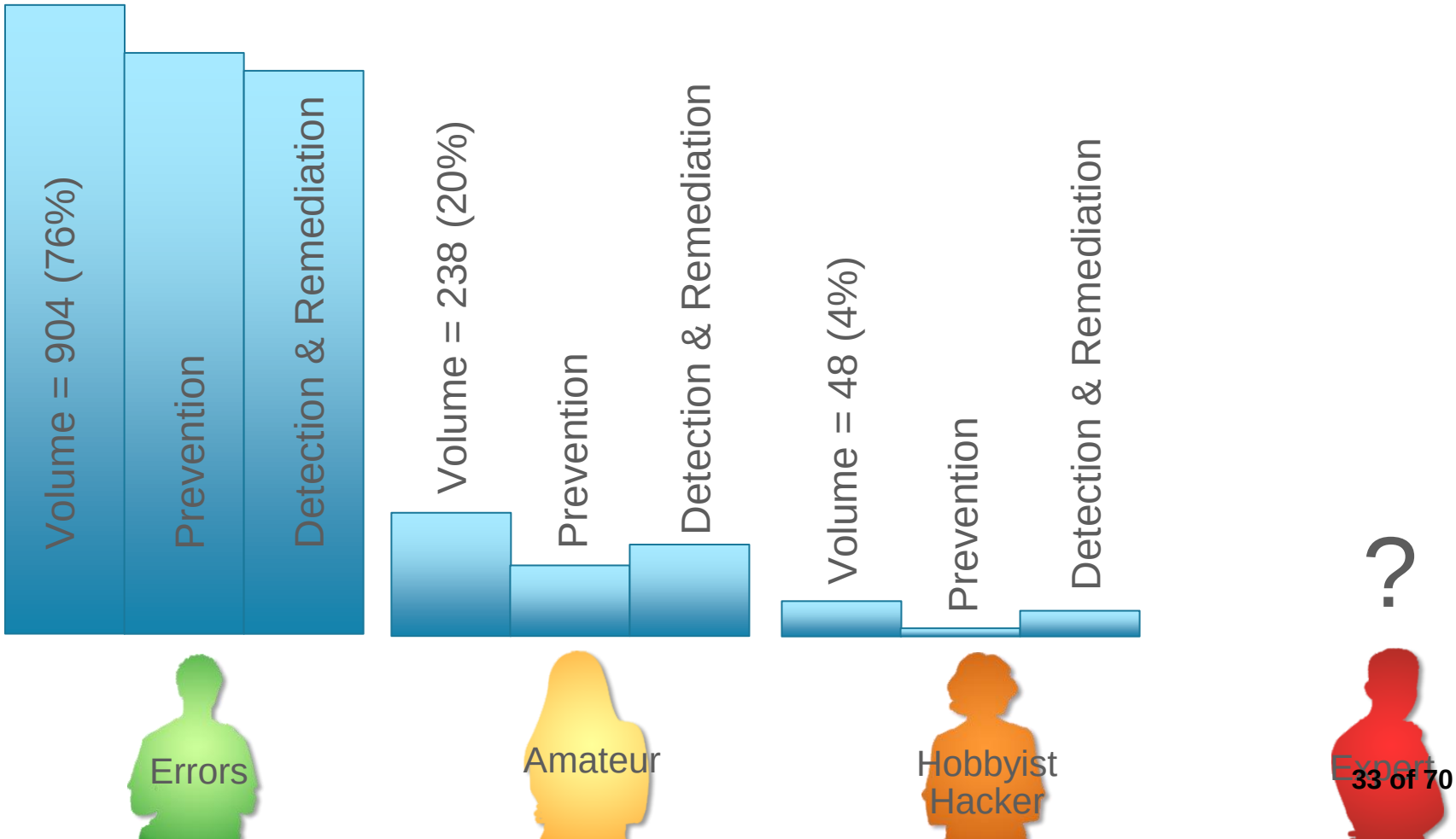
IT@UMN

AVERAGE UMN INCIDENTS BY ADVERSARY TYPE

Average # of Information Security Incidents per Month:

1,190

In FY13, we had 29 Breaches resulting in the loss of 3,836 records



IT@UMN

We Closely Track Peer Institutions

Institution	When	Records Lost
University of Nebraska	June 2012	654,000
University of North Carolina	May 2012	350,000
Arizona State University	January 2012	300,000
NW Florida State College	October 2012	279,000
Indiana University	February 2014	146,000
University of Maryland	February 2014	287,580
North Dakota University System	March 2014	291,465

2.3 Million Since 2012

and counting….

Source: Privacy Rights Clearinghouse
www.privacyrights.org

IT@UMN

Let's Review Some Recent Examples…

- Target
- University of Maryland
- IRS Fraud at Big10 Schools
- UMN Examples
  - Errors
  - Amateur
  - Advanced Persistent Threat (Expert)

IT@UMN

WHAT HAPPENED AT TARGET?

- A Target HVAC vendor was *spear phished*
- Zeus (a common *malware*) was used to steal passwords
- With those passwords, attackers gained access to the Point of Sale network
- Attackers installed a simple memory scraper
- Adversary Type: Expert

- **These simple steps led to a breach of:**
  - **40 million credit cards**
  - **70 million records of personal information**

IT@UMN

WHAT HAPPENED AT THE UNIVERSITY OF MARYLAND?

- Attacker compromised the digital identity system (LDAP directory)
- Passwords of several IT staff were reset
- Attacker used compromised IT staff credentials to access a database
- Entire attack and theft *took less than 30 minutes*
- Adversary Type: Expert

- **Database contained 300,000 records including student and staff:**
  - **Names**
  - **Social security numbers**
  - **Date of births**

IT@UMN

IRS Fraud at BIG TEN SCHOOLS

About half the Big Ten Universities have had users hit with false IRS claims cyber attack (criminal submitting false tax returns):

- One university had more than 200 false claims
- All it takes a SSN and a *roughly* correct spelling of the name
- Tax refunds below a certain threshold are paid prior to review by the IRS

IT@UMN

UMN EXAMPLE:

Stolen Hard Drive

- A faculty member's laptop and external hard drive were stolen from an unlocked location:
  - Contained a primary copy of highly-sensitive criminal / victim information from Hennepin and Ramsey counties
  - External Hard Drive provided a back-up copy
  - Both devices were stored in same location
- Resulted in breach notifications to 349 individuals

Webserver Posting

- Data were inadvertently posted on a webserver
- Data contained 430 records of names, address, phone number, and social security numbers

Email Sending Mistake

- Advisor mistakenly emailed an attachment to 53 graduating seniors containing 448 degree candidates
- Personal information included: name, ID, GPA, major, advisor and email address

IT@UMN

UMN EXAMPLE:

System Administrator Spamming

- A system admin's credentials were stolen while wirelessly checking email on a mobile device:
  - Incident was reported to Information Security when he could not access his account
  - Upon account access, the system admin noticed a high number of sent items
  - Compromised email account was being used for email spamming
- Forensics analysis determined that no private information was breached during the incident

IT@UMN

UMN Example: National Interest (Advanced Persistent Threat)

National Center for Food Protection and Defense

- Sourced from China
- Used an unprotected multifunction printer
  - Data transfers to China went unnoticed for months
  - Undetected by the University / Notified by FBI

Normal Security Controls Ineffective

- No incident reported (no affected users)
- No malware detected
- Low, slow data transfers were normal (Intrusion Detection)

IT@UMN

Current UMN Security Efforts for detection, Response and prevention

Detection & Response

- Log Management
- Incident Management
- Breach Management
- Intrusion Detection
- Forensics

Prevention

- Security Awareness
- Anti-Virus
- Vulnerability Management
- System & Communication Encryption
- Identity & Access Management
- Security Risk Management

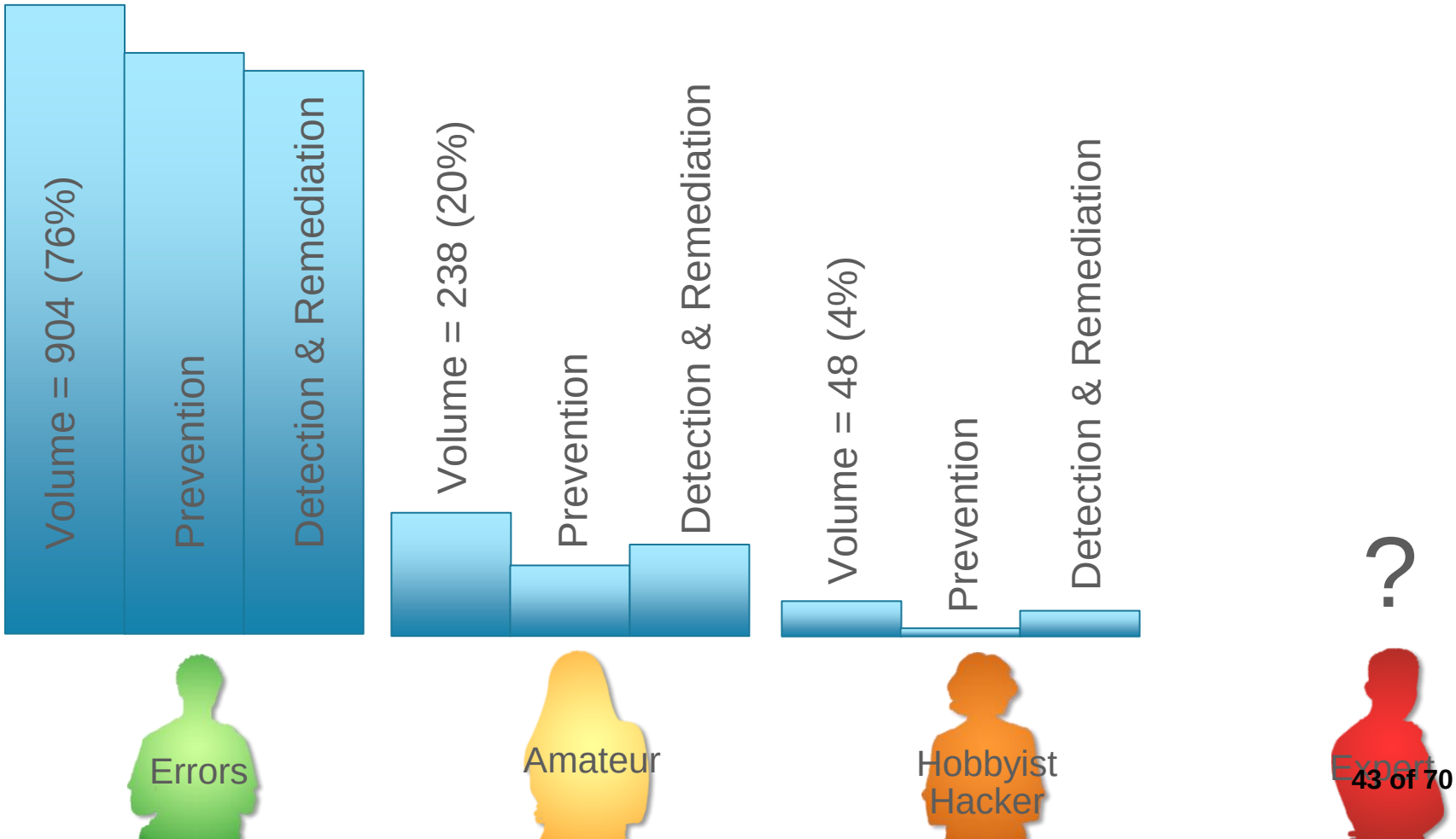
IT@UMN

AVERAGE UMN INCIDENTS BY ADVERSARY TYPE

Average # of Information Security Incidents per Month:

1,190

In FY13, we had 29 Breaches resulting in the loss of 3,836 records



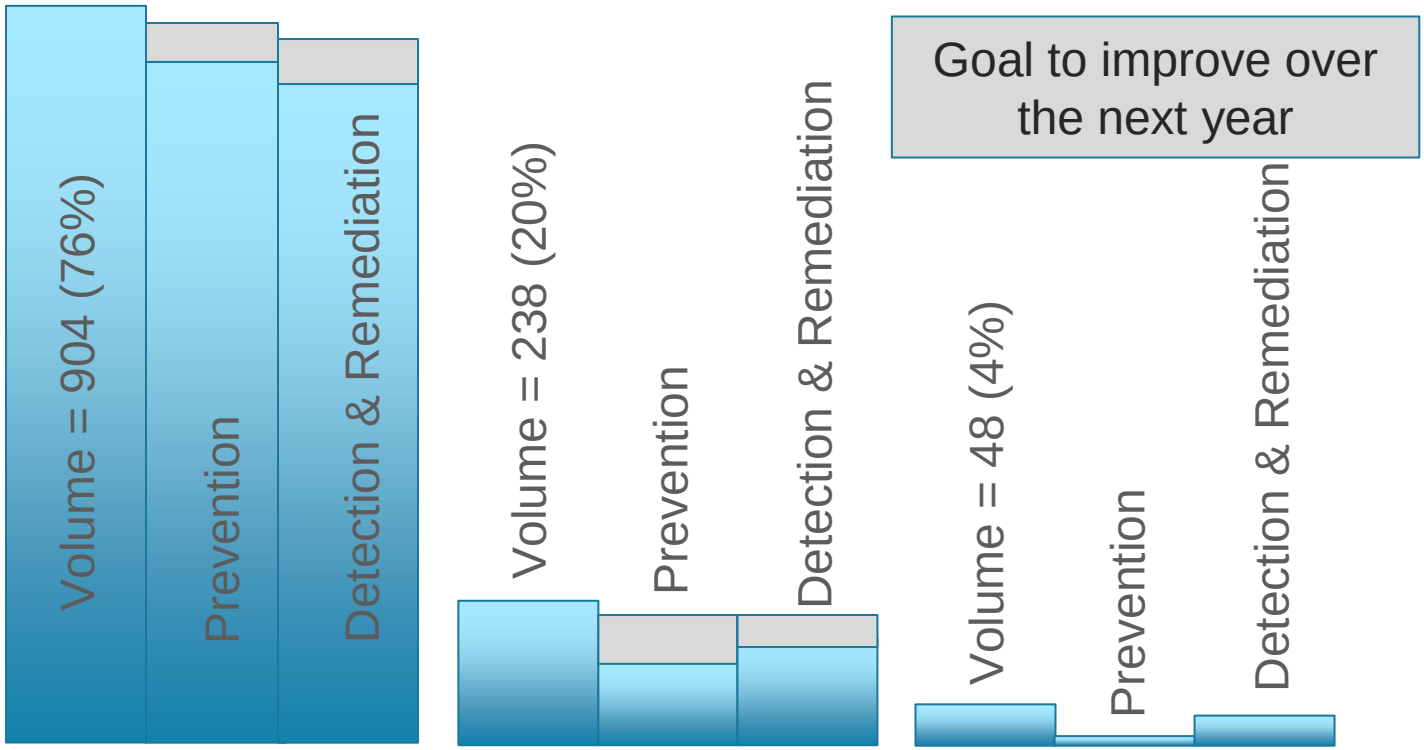
IT@UMN

Average UMN Incidents by Adversary Type

Average # of Information Security Incidents per Month:

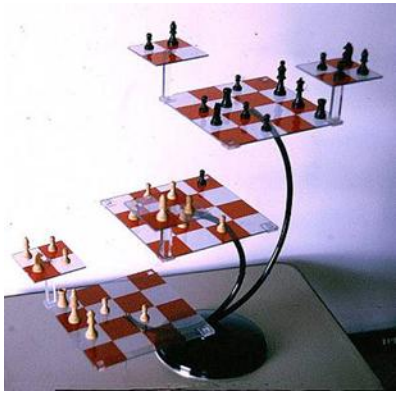
1,190

In FY13, we had 29 Breaches resulting in the loss of 3,836 records



IT@UMN

THE SIGNIFICANT SECURITY CHALLENGE



- Our existing Information Security controls provide due diligence to:
  - reduce the frequency of security breaches, and
  - 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.
- A high-impact security breach **will** occur.
- And expert security incidents will remain undetected, regardless of the security controls implemented.

IT@UMN

THANK YOU!

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 11, 2014**

Agenda Item: Internal Audit Update

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

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

Presenters: Gail Klatt, Associate Vice President

Purpose & Key Points

To update the Audit Committee on internal audit activities, results, and observations, and assist the committing in fulfilling its fiduciary responsibilities as defined by Board of Regents Policy: *Audit Committee Charter*. Updates include:

- Since our last follow-up at the June 2014 meeting, University departments implemented 23% of the outstanding recommendations rated as "essential". This is less than our expected implementation rate of 40%. Three units fully implemented all their remaining "essential" recommendations.
- An updated control evaluation chart is included for each audit to show progress made on the "essential" items.
- Six audit reports containing three recommendations rated as "essential" were issued in the last three months.

Background Information

This report is prepared three times per year and is presented to the Audit Committee in conformance with Board of Regents Policy: *Board Operations and Agenda Guidelines.*

Internal Audit Update

University of Minnesota Regents Audit Committee
September 11, 2014

This report includes:

- Audit Observations/Information/Status of Critical Measures/Other Items
- Status of "Essential" Recommendations & Bar Charts Showing Progress Made
- Audit Activity Report
- Audit Reports Issued Since June 2014

Details for any of the items in this report are available on request. Individual reports were sent to the President, Provost, Vice Presidents, and Chancellors about these internal audit issues.

Audit Observations/Information

Status of Critical Measures

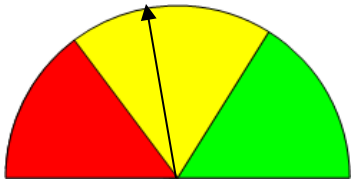
As part of our on-going efforts to provide the Audit Committee with critical information in as concise a format as possible, we have developed the following three charts to present a "snap-shot" status report on work performed by the Office of Internal Audit.

The first chart, "Essential Recommendation Implementation", provides our overall assessment of the success University departments had during the last quarter in implementing our essential recommendations. Readings in the yellow or red indicate implementation percentages less than, or significantly less than, our expected University-wide rate of 40%. Detailed information on this topic, both institution-wide and for each individual unit, is contained in the next section of this Update Report.

The second chart, entitled "Progress Towards Annual Audit Plan Completion", is our assessment of how we are progressing towards completion of the FY 2015 Annual Audit Plan. Readings less than green could be influenced by a variety of factors (i.e. insufficient staff resources; increased time spent on non-scheduled audits or investigations).

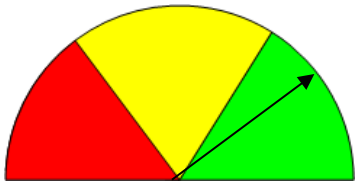
The final chart, "Time Spent on Investigative Activities", provides a status report on the amount of time consumed by investigative activities. Our annual plan provided an estimated budget for this type of work, and the chart will indicate if we expect that budget to be sufficient. Continued readings in the yellow or red may result in seeking Audit Committee approval for modifying the Annual Audit Plan.

Essential Recommendation Implementation



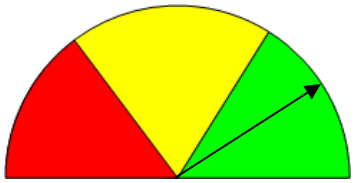
Implementation rates were 23% for the period, less than our expected rate of 40%.

Progress Towards Annual Audit Plan Completion



Time spent to date on the FY 2015 audit plan is about what was expected and budgeted for the year to date. One vacant IT auditor position is in the process of being filled.

Time Spent on Investigative Activities



Time spent on investigative activities and special projects is about what was expected and budgeted for the year to date.

Other Items

- As part of our continuous improvement efforts the Office of Internal Audit has updated the format of its audit reports. The Executive Summary is now a document separate from the main audit report, and report recipients will receive both documents when the report is issued. We appreciate the guidance provided by University Relations as we developed these new documents.

- Professional standards require that every five years internal audit organizations receive an independent review and assessment of their operations and practices to measure compliance with internal auditing standards. Office of Internal Audit staff are currently in the midst of performing our internal self-assessment. A team of four external reviewers has been selected that will conduct the formal quality assurance review, which is scheduled for February 2015.

Status of "Essential" Recommendations as of August 29, 2014

Report Date	Audit **(P) *Indicates a University process audit***	Original Report Control Rating	# of Essential Recommendations in the Report	# of Essential Recommendations Remaining From Prior Quarter	Current Quarter Results					Overall Progress Towards Implementation*
					Implemented	Partially Implemented		Not Implemented		
						Not Past Target Date	Past Target Date	Not Past Target Date	Past Target Date	
Audits > 2 years old (see the following report for details on unresolved issues)										
Oct-11	UMD School of Fine Arts	Adequate	10	2			1		1	Satisfactory
Nov-11	**Intercollegiate Athletics**	**Needs Improvement**	**5**	**2**	**2**					**Completed**
Feb-12	Dentistry - axiUm System (P)	Adequate	14	2	1		1			Satisfactory
Feb-12	**University Contract Management (P)**	**Adequate**	**17**	**1**	**1**					**Completed**
Audits < 2 years old; have received prior follow-up										
Dec-12	Network Segments Not Managed By OIT	Adequate	5	5	3		2			Satisfactory
May-13	Travel & Employee Reimbursements (P)	Good	1	1			1			Satisfactory
May-13	UMD - College of Liberal Arts	Adequate	6	2		2				Satisfactory
Jun-13	Research Data Storage (P)	Adequate	5	2			2			Satisfactory
Dec-13	UMD Information Tech. Systems & Services	Good	6	4		3	1			Satisfactory
Jan-14	**Department of Chemistry**	**Good**	**2**	**1**	**1**					**Completed**
Feb-14	University-wide Purchasing Process (P)	Good	2	2			1	1		Satisfactory
Audits receiving first-time follow-up										
Apr-14	UM - Crookston Campus	Good	6	6	4	1	1			Satisfactory
Apr-14	CLA East Bank 1 Financial Services Team	Good	1	1			1			Satisfactory
May-14	UMD Parking Services	Good	1	1			1			Satisfactory
Jun-14	Identity Management	Needs Improvement	11	11		6	2	3		Satisfactory
Jun-14	Parking & Transportation Services	Adequate	10	10		10				Satisfactory
	Total:		**102**	**53**	**12**	**22**	**14**	**4**	**1**	

* The following bar charts provide details on progress made towards implementation

"Essential" Recommendation Implementation Trends

Month / Year of Follow-up Report

	Sept. 2014	June 2014	Feb. 2014	Sept. 2013	June 2013	Feb. 2013	Sept. 2012	June 2012	Feb. 2012	Average
# of Essential Recommendations Receiving Follow-up	53	34	36	64	56	67	72	89	82	61
# of Recommendations Considered Fully Implemented	12	10	13	30	13	26	16	26	55	22
Implementation Percentage	23%	29%	36%	47%	23%	39%	22%	29%	67%	36%

Current Status of Recommendations Rated as "Essential" That Are Over Two Years Old and Are Not Fully Implemented

Audit/ Report Date	***Status-Partially Implemented (P) or Not Implemented (N)***	***Senior Management Contact***	***Summary of the Issue/Risk Involved***	***Current Comments From Management***
UMD School of Fine Arts Oct-11	P	William Payne Bilin Tsai	Glensheen should update and expand its inventory records with the ultimate goal of having a complete record of the entire collection. Periodically, the presence and location of inventory items should be verified on at least a sample basis.	According to the interim director of Glensheen, the physical inventory is now underway. All prior physical files have been entered into a collections management system. The longer process of identifying the pieces yet to be included throughout the mansion will begin next week.
	N	William Payne Bilin Tsai	Glensheen management should work with Accounting Services to develop procedures for reporting the value of its collection.	Efforts to appraise the collection will commence after the inventory has been completed.
# of Items 2				
Dentistry - axiUm System Feb-12	P	Jeff Ogden Leon Assael	Dentistry should investigate the $8,642 difference between axiUm accounts receivable and the general ledger. Going forward, the reconciliation between axiUm accounts receivable to the general ledger should be completed monthly. Any errors or reconciling items should be investigated and corrected timely. Oversight to ensure completeness and timeliness of reconciliations should be established. Discrepancies between the axiUm aging report and the patient detail accounts should also be investigated. Dentistry should determine whether any processes (i.e., held payments, unapplied adjustments, etc.) need to be modified based upon their findings.	The new custom axiUm AR report and pivot tables, which were designed for more accurate and efficient calculation of production numbers and verification of calibration between axiUm and PS AR is working well. Starting with April, 2014 AARF forms were and are being completed monthly. Bad debt is being entered into PS and reported to Mr. David Laden monthly. Cash is being fully reconciled throughout the month (instead of at the end of the month) and identified problems are immediately investigated. The standard is to correct errors by the end of the month; if they are not corrected they are carried over and an explanation should be given about who is resolving it. The manager reviews carried forward reconciling items for timely resolution. Unreconciled items found by the consultant are taking more time to resolve than we were led to believe and work continues on that front. To address this situation, our new reconciler, who had other duties, is being allowed to work on the reconciliation full-time for as long as it takes to clear the older reconciling items. The manager has not yet performed a full reconciliation on his own, however, at this time he is able to get the productivity numbers for PeopleSoft. Closer tracking of refunds has been accomplished – they are entered into EFS with a CF2. We worked closely with Central A/R to ensure a smooth year-end reconciliation and closing. We implemented a desirable new method to track unearned income and refund liability.
# of Items 1				

Total: 3

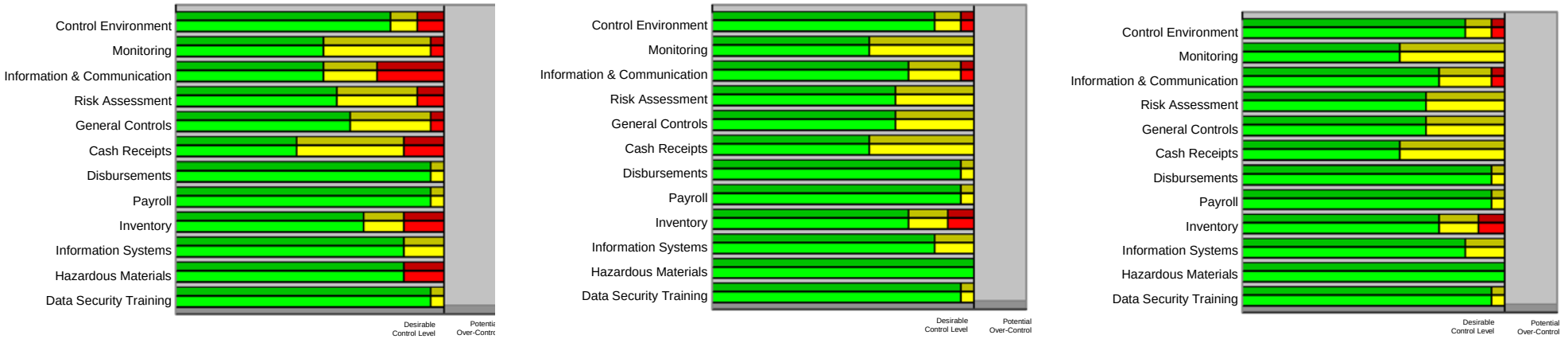
The bar charts shown below are presented to provide pictorial displays of the progress units are making on implementing audit recommendations rated as "essential". The bar chart included in the original report is shown in the left column, along with updated bar charts showing the previous quarter and the current status of the "essential" recommendations only (those bars that have red segments). The chart in the center column displays the status as of June 2014, while the chart on the right represents the current status. Charts are not presented for investigations. Charts for those units having implemented all "essential" recommendations during the current quarter are shown at the end of this report.

Original Report Evaluation

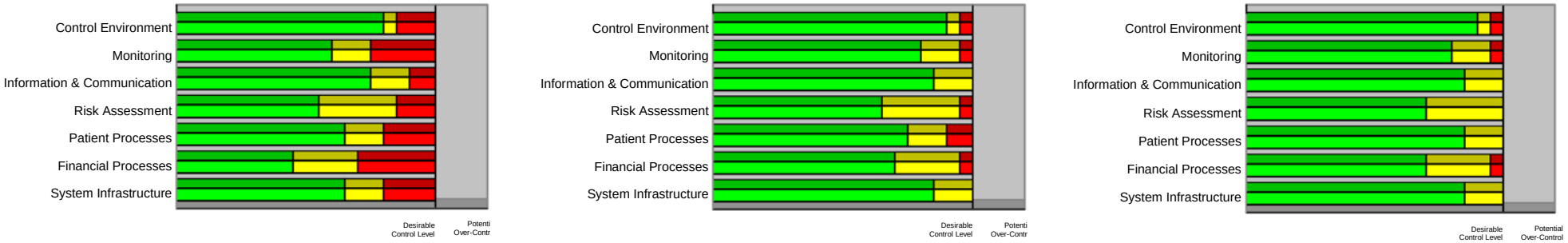
Previous Quarter Evaluation

Current Quarter Evaluation

U of MN Duluth - School of Fine Arts (October 2011)



Dentistry - axiUm (February 2012)



Adequate Control

Significant Control Level

Critical Control Level

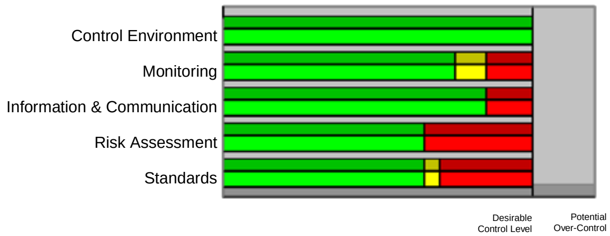
Potential Over-Control

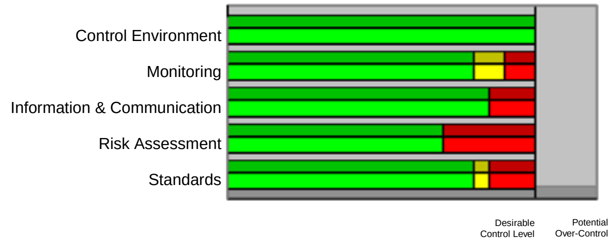
Original Report Evaluation

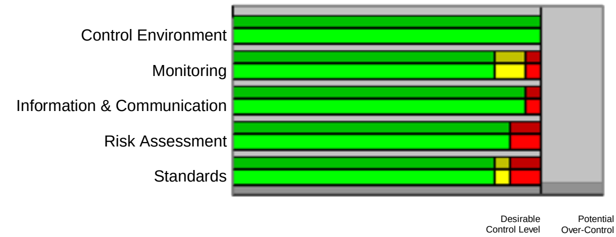
Previous Quarter Evaluation

Current Quarter Evaluation

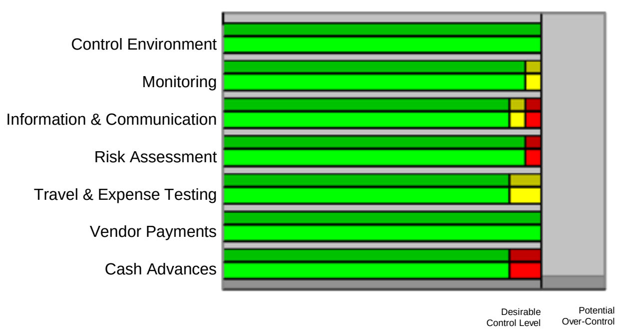
Network Segments Not Managed By OIT (December 2012)

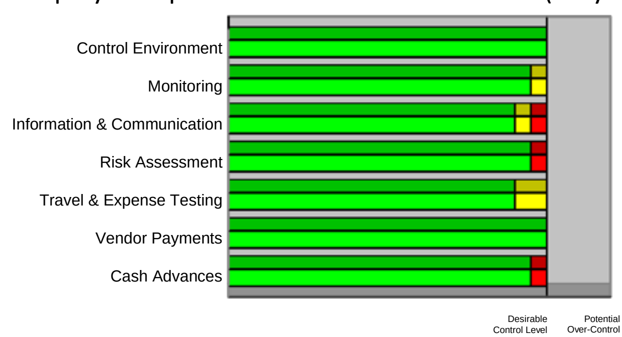


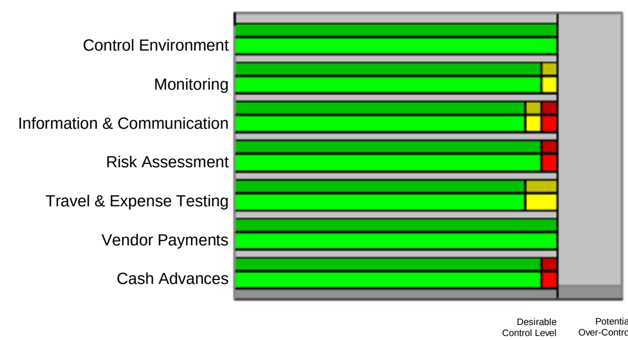




Travel & Employee Expense Reimbursement Process (May 2013)







Adequate Control

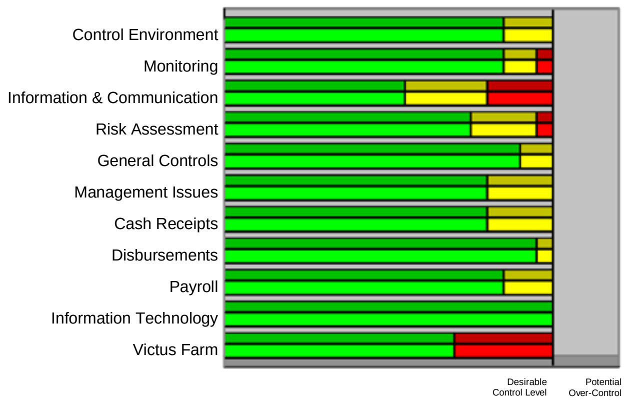
Significant Control Level

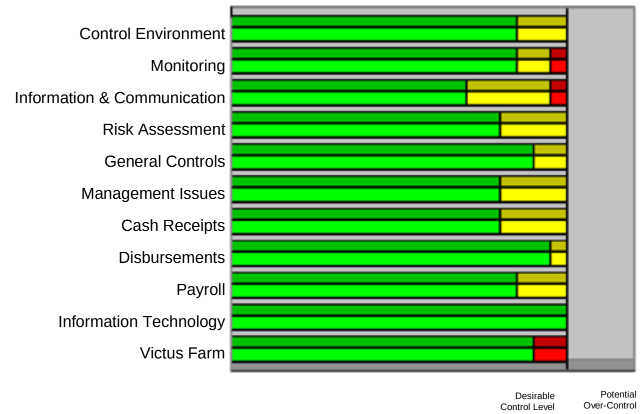
Critical Control Level

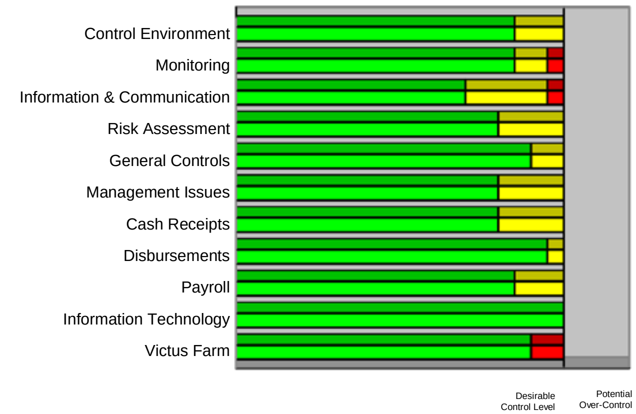
Potential Over-Control

Original Report Evaluation | Previous Quarter Evaluation | Current Quarter Evaluation

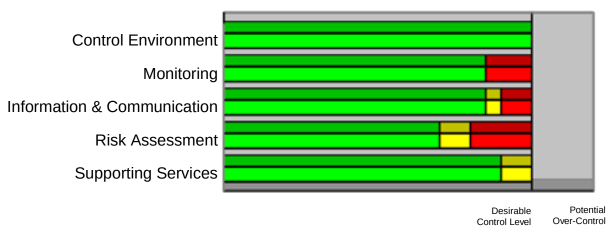
U of MN Duluth - College of Liberal Arts (May 2013)

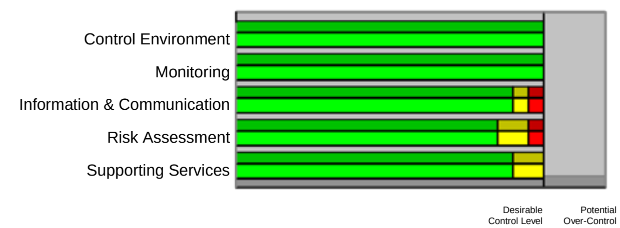






Research Data Storage (June 2013)

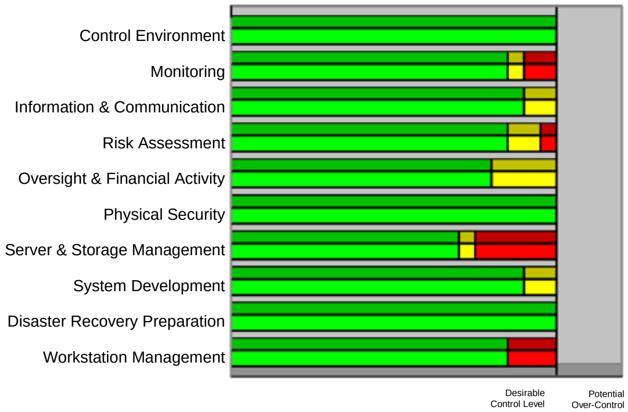


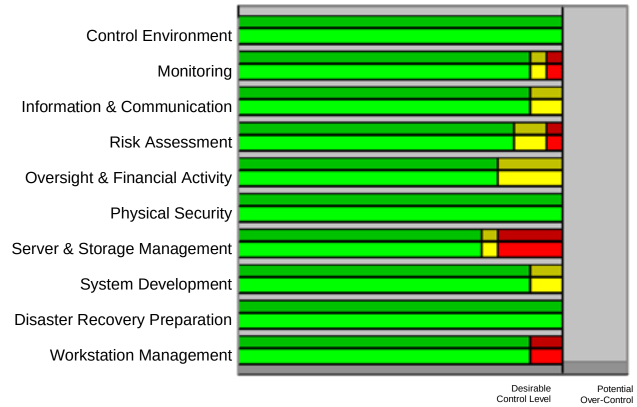


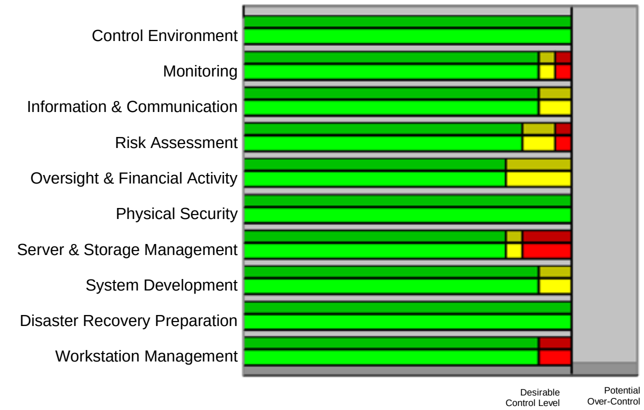
Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

Original Report Evaluation | Previous Quarter Evaluation | Current Quarter Evaluation

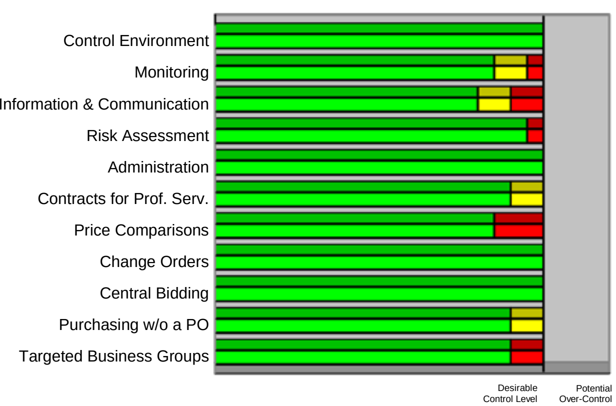
U of MN Duluth - Information Technology Systems and Services (December 2013)

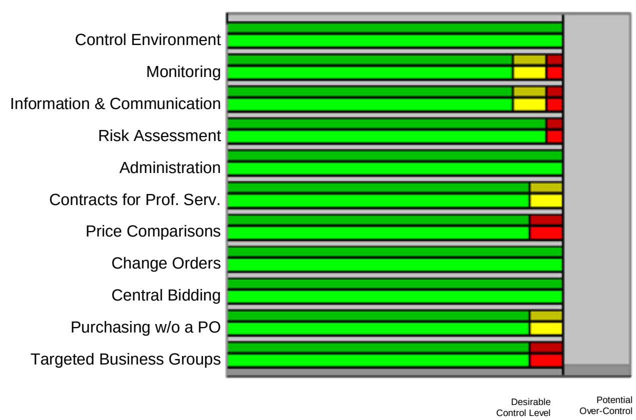


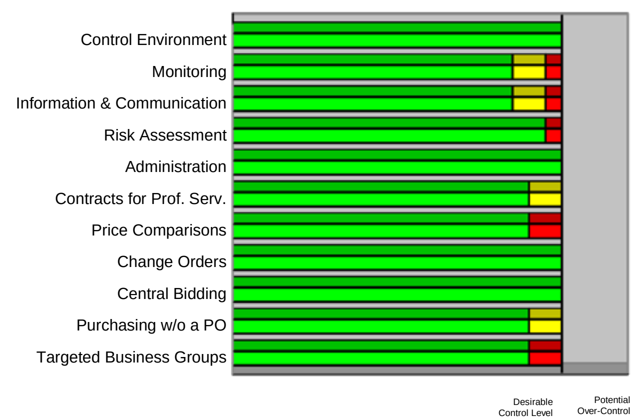




University-wide Purchasing Process (February 2014)



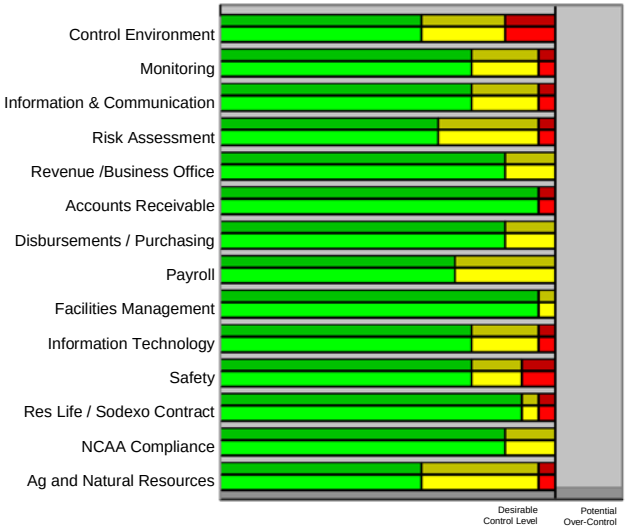




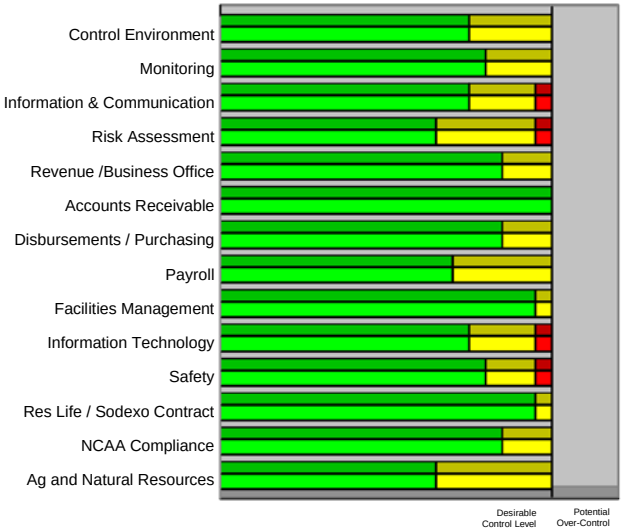
Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

Original Report Evaluation | Previous Quarter Evaluation | Current Quarter Evaluation

UM - Crookston Campus (April 2014)

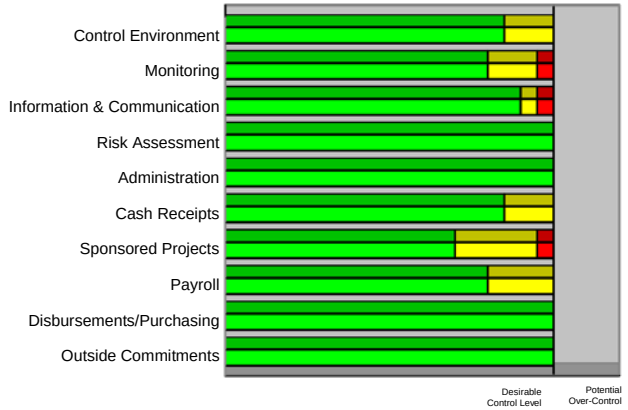


NO PREVIOUS CONTROL EVALUATION CHART



College of Liberal Arts, East Bank 1 Financial Services Team (April 2014)

NO PREVIOUS CONTROL EVALUATION CHART



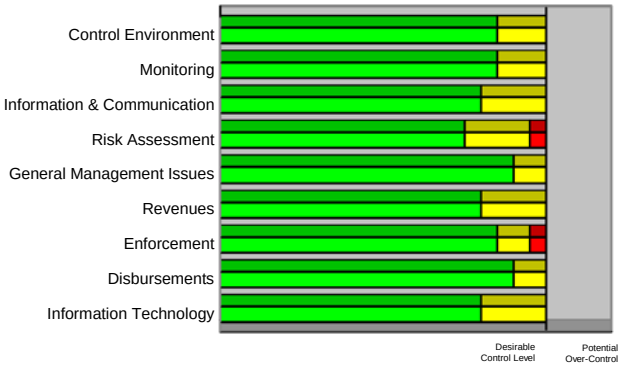
Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

Original Report Evaluation

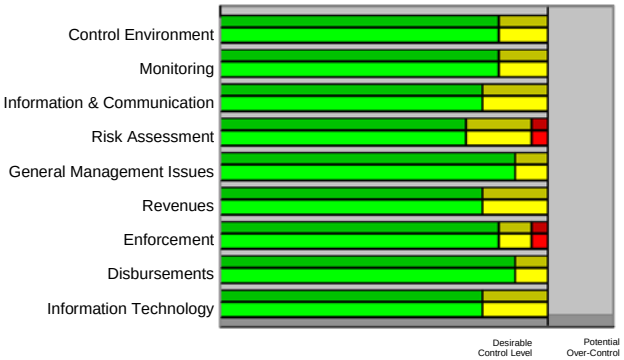
Previous Quarter Evaluation

Current Quarter Evaluation

UMD Parking Services (May 2014)

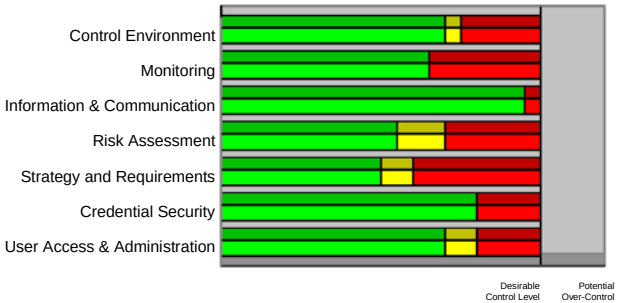


NO PREVIOUS CONTROL EVALUATION CHART



Identity Management (June 2014)

NO PREVIOUS CONTROL EVALUATION CHART



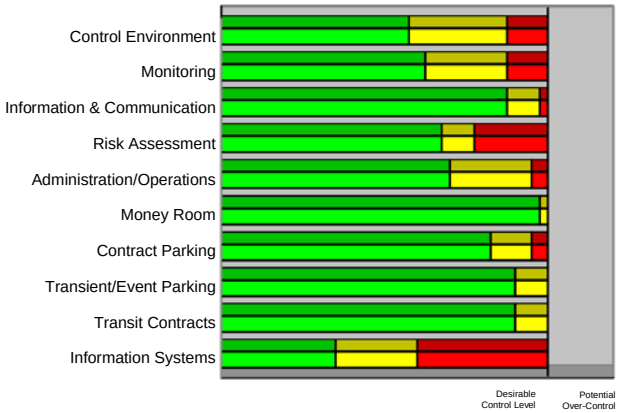
Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

Original Report Evaluation

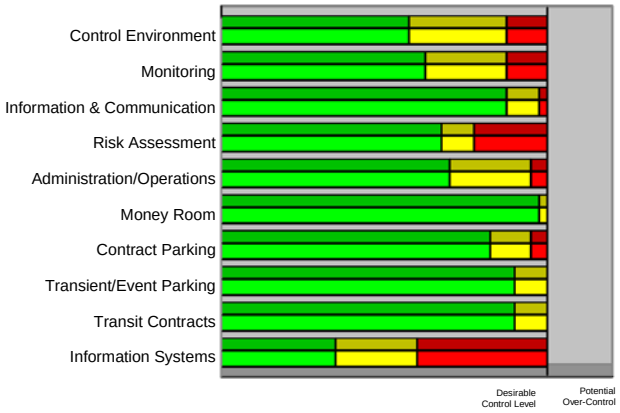
Previous Quarter Evaluation

Current Quarter Evaluation

Parking and Transportation Services (June 2014)



NO PREVIOUS CONTROL EVALUATION CHART



Adequate Control

Significant Control Level

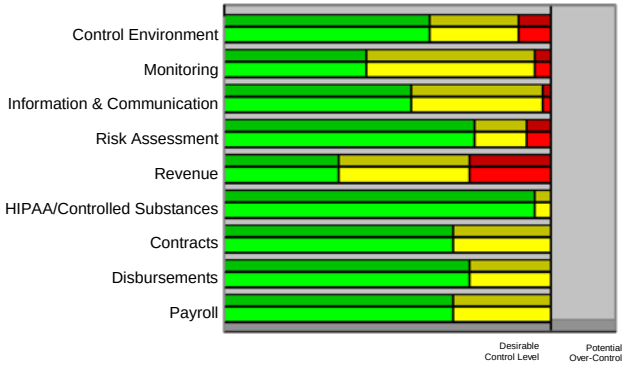
Critical Control Level

Potential Over-Control

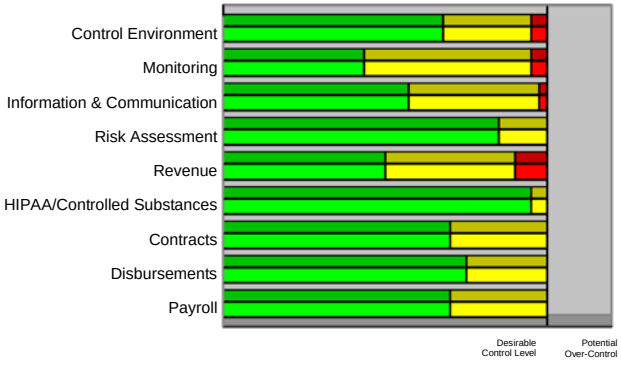
Units with Charts that Fully Implemented their "Essential" Recommendations During the Past Quarter

Intercollegiate Athletics (November 2011)

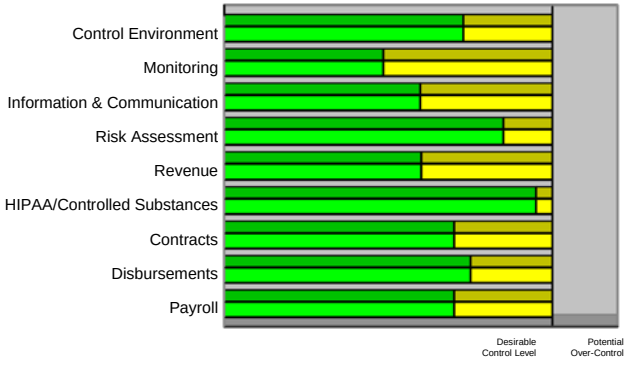
Original Report Evaluation



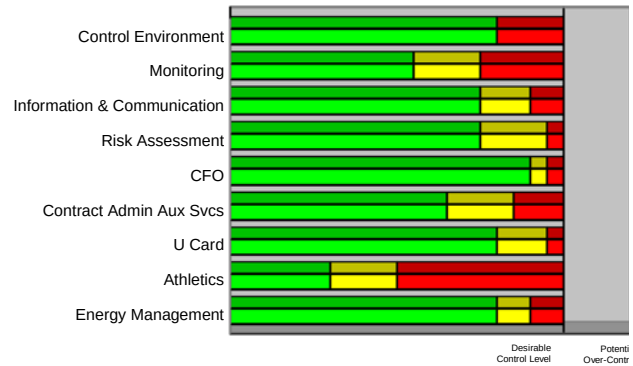
Previous Quarter Evaluation

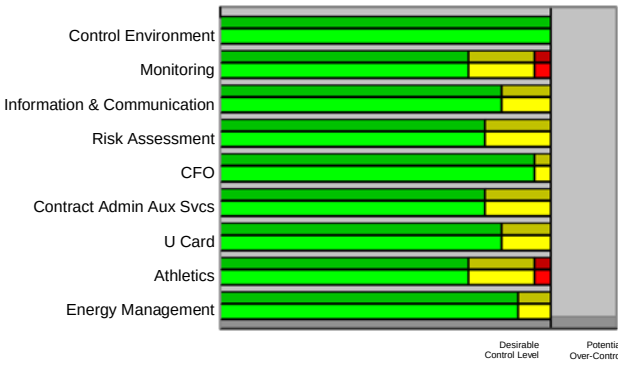


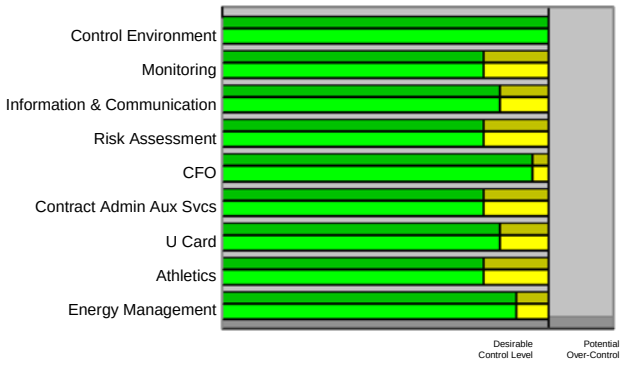
Current Quarter Evaluation



University Contract Management (February 2012)







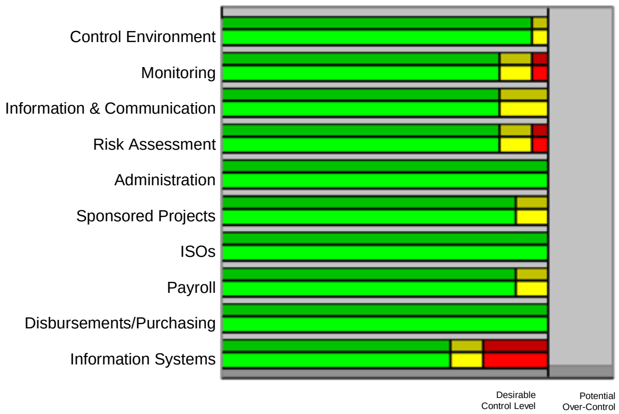
Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

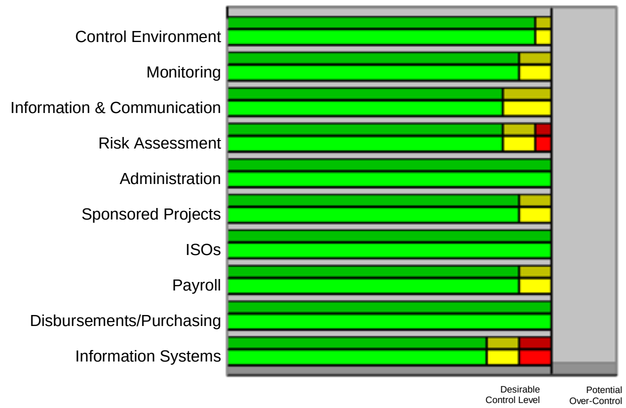
Original Report Evaluation

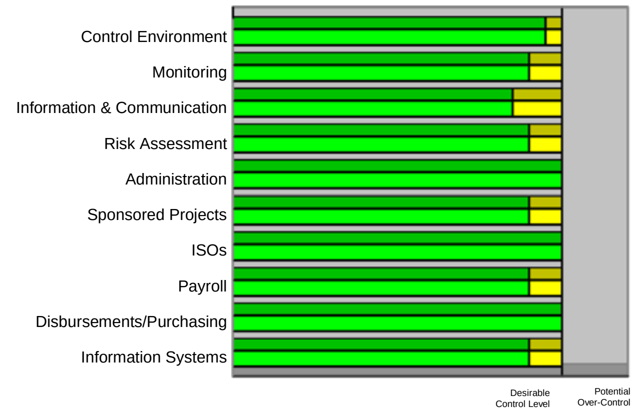
Previous Quarter Evaluation

Current Quarter Evaluation

Department of Chemistry (January 2014)







Adequate Control | Significant Control Level | Critical Control Level | Potential Over-Control

Audit Activity Report

Scheduled Audits

- Completed audits of the new U-wide cash depositing process, the vendor file maintenance process, the U Market procurement process, Minnesota Sea Grant and Research Animal Resources. Details are shown on the following charts.

- Began/continued audits of: University Recreation & Wellness, Hormel Institute, Athletics Aspire contract, Medical School Duluth campus, new technology due diligence, the processes being used to develop and implement the University's grading system upgrade, physical security of server rooms, top University researchers, Carlson School of Management and the Clinical Translational Sciences Institute (CTSI).

- Continue to monitor ESUP readiness for implementation.

Non-Scheduled Audits

- Completed a requested audit of the UMD University for Seniors program. Details are shown on the following chart.

- Continued a requested audit of the St. Anthony Falls Lab NSF Renovation Grant and issued a draft report to management.

- Began a requested audit of the Athletics Baseline Tennis Center

Investigations

- Performed investigative work on nine issues in accordance with the University Policy on Reporting and Addressing Concerns of Misconduct.

Special Projects

- Provided consulting services related to University payroll exception testing and Boynton Health Service accounts receivable reconciling processes.

- Participated in RFP reviews for external assessments of HIPAA Security and the University's IT data security program.

Other Audit Activities

- Participated in the following:
  - Senior Leadership Group
  - Operational Excellence Leadership Team
  - President's Policy Committee
  - Board of Regents Policy Committee
  - Executive Compliance Oversight Committee
  - Institutional Conflict of Interest Committee
  - University of Minnesota Foundation Audit Committee
  - Fairview Health Systems Audit Committee
  - Enterprise System Upgrade - Human Resource Functional Steering Committee
  - Uniform Guidance Steering Committee
  - IT Leadership Community of Practice

Audit Reports Issued Since June 2014

UMD University for Seniors

Report #	1501	Issue Date	Jul-14
# of Essential Recs.	2	Total # of Recs.	10
Overall Assessment	Good	Adequacy of MAP	Satisfactory

University for Seniors is a membership-based organization of persons age 50 and older. Its purpose is to provide intellectual and cultural stimulation and growth, thus enhancing life experiences for its members. In our opinion, the operational and financial controls over most functions within University for Seniors are generally effective; however, improvement is needed in endowment management.

U-Wide Cash Depositing Process

Report #	1502	Issue Date	Aug-14
# of Essential Recs.	0	Total # of Recs.	0
Overall Assessment	Good	Adequacy of MAP	NA

Results of the audit work performed show that the Office of Investments and Banking (OIB), in conjunction with the Treasury Accounting unit within the Controller's Office, have developed a control environment and system of internal control that addresses the major business and compliance risks governing this process. In addition, we found good University-wide compliance in the units we tested regarding compliance with this revised process and the accompanying policies.

Vendor File Maintenance Process

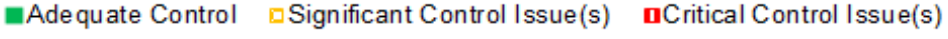
Report #	1503	Issue Date	Aug-14
# of Essential Recs.	0	Total # of Recs.	0
Overall Assessment	Good	Adequacy of MAP	NA

Results of the audit work performed show that the Vendor File Maintenance process has a control environment and system of internal control that addresses most major business risks. However, Disbursement Services was provided with a list of possible enhancements they may wish to consider implementing as additional best practices and to further minimize possible fraud risks. These include reviewing the approval process currently used for vendor set-ups and changes, establishing a set timeframe after which vendors with no financial activity should be moved to an "inactive" status, and improving monitoring activities related to the vendor file.

U Market Procurement Process

Report #	1504	Issue Date	Aug-14
# of Essential Recs.	0	Total # of Recs.	14
Overall Assessment	Good	Adequacy of MAP	Satisfactory

U Market is a key component of the University's strategic sourcing initiative. Implementing U Market was one of the first significant Operational Excellence initiatives. Results of the audit work performed show that U Market, a joint effort between the University Controller's Office (Purchasing Services) and Auxiliary Services (U Market Services) has developed a control environment and system of internal control that addresses most major business and compliance risks. However, improvement is needed in areas related to: shipping charges, oversight of the U Market eProcurement system's vendor, administrator access rights, the merchandise credit/return process, and controls and processes pertaining to external customers.



Minnesota Sea Grant

Report #	1505	Issue Date	Aug-14
# of Essential Recs.	1	Total # of Recs.	7
Overall Assessment	Good	Adequacy of MAP	Satisfactory

Minnesota Sea Grant's mission is "To facilitate interaction among the public and scientists to enhance communities, the environment and economies along Lake Superior and Minnesota's inland waters by identifying information needs, fostering research, and communicating results." We believe Minnesota Sea Grant has developed a control environment and a system of internal control that addresses most major business, compliance, and information technology risks. However, improvement is needed in areas pertaining to overtime/compensatory time policies and procedures, external sales, cash receipts, and inventory.

Research Animal Resources

Report #	1506	Issue Date	Aug-14
# of Essential Recs.	0	Total # of Recs.	10
Overall Assessment	Good	Adequacy of MAP	Satisfactory

The mission of RAR is to provide for the care, health, and well-being of animals used for research and education at University of Minnesota; to administer to the animal related needs of University researchers and educators through dissemination of knowledge and resources and; to serve the public by ensuring observance of all legal and ethical standards pertaining to the use of animals for research and education at the University of Minnesota. Based on the results of our review we believe RAR's processes are well designed and operate effectively to support animal housing at the University. However, the WDS system that aids in RAR's ability to be effective lacks some controls and will not be supported in the near future.

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 11, 2014**

Agenda Item: Office of Internal Audit Charter: *Department Charter*

X	**Review**	☐	**Review + Action**	☐	**Action**	☐	**Discussion**

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

Presenters: Gail Klatt, Associate Vice President

Purpose & Key Points

According to Board of Regents Policy: *Audit Committee Charter*, the Audit Committee is responsible for providing oversight of the internal audit function, including reviewing and approving any changes to the function's charter. The proposed changes are intended to maintain alignment with professional standards and guidance.

Background Information

The internal audit charter was last reviewed by the Audit Committee in July 2008.

CHARTER

Misson and Scope of Work

The mission of the Office of Internal Audit is to provide independent, objective assurance and advisory services designed to add value and improve the operations of the University of Minnesota. It helps the University accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. It strives to enhance and protect institutional value by providing stakeholders with risk-based, objective and reliable assurance, advice, and insight.

The scope of work of the Office of Internal Audit is to determine whether the University of Minnesota's network of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction between governance groups occurs as needed
- Important financial, managerial, and operating information is accurate, reliable, and timely.
- Employees' actions are in compliance with policies, standards, procedures, and applicable laws and regulations.
- Resources are acquired economically, used efficiently, and protected adequately.
- Programs, plans, and objectives are achieved.
- Quality and continuous improvement are fostered in the University's control process.
- Significant legislative or regulatory issues impacting the University are recognized and addressed appropriately.

The Office of Internal Audit considers risks broadly and includes within its scope all activity posing financial, operational, technological, regulatory or reputational risk to the University. Opportunities for improving management control, efficiency and the University's image may be identified during audits. They will be communicated to the appropriate level of management.

Accountability

The Director of the Office of Internal Audit, in the discharge of his/her duties, is accountable to the Board of Regents Audit Committee and the President to:

- Provide assessments on the adequacy and effectiveness of the University's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.

- Report significant issues relating to the processes for controlling University activities including potential improvements to those processes.
- Reporting the acceptance of risk by the administration, as appropriate.
- Provide information concerning outstanding issues through their resolution.
- Periodically provide information on the status and results of the annual audit plan and the sufficiency of department resources.
- Coordinate efforts with other control and monitoring functions (e.g., compliance, security, legal environmental, external auditors, etc.).

Independence

To provide for the independence of the Office of Internal Audit, the Board of Regents delegates directly to the Director of the Office of Internal Audit the authorities necessary to perform the duties set forth in the mission and scope of work. Additionally, the Director of the Office of Internal Audit is delegated administrative and operational authorities by the President of the University. The Office of Internal Audit is to be free from undue influence in the selection of activities to be examined and the audit techniques and procedures to be used.

Responsibility

The Director and staff of the Office of Internal Audit are responsible for:

- Developing a flexible annual audit plan using an appropriate risk based methodology, including any risks or control concerns identified by management, and submitting that plan to the audit committee for review and concurrence, as well as providing periodic updates as to the status of the plan.
- Implementing the annual audit plan, as approved, including any special tasks or projects requested by management and the audit committee.
- Maintaining a professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this Charter.
- Maintaining an audit quality review program that promotes the continuous improvement of the internal audit practice including periodic assessment by independent external resources.
- Considering the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the University at a reasonable overall cost.
- Issuing periodic reports to the audit committee and management summarizing results of audit activities.
- Keeping the audit committee informed of emerging trends and successful practices in internal auditing.
- Conducting investigations of allegations of financial and operational misconduct

Authority

The Director and staff of the Office of Internal Audit are authorized to:

- Have unrestricted access to all University functions, records, property, and personnel, subject to state and federal law.
- Have full and free access to the audit committee.
- Allocate departmental resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives.
- Obtain the necessary assistance of personnel in units of the University where they perform audits, as well as other specialized services from within or outside the institution.

The Director and staff of the Office of Internal Audit are not authorized to:

- Perform any operational duties for the University.
- Initiate or approve accounting transactions external to the Office of Internal Audit.
- Direct activities of any University employee not employed by the Office of Internal Audit, except to the extent such employees have been appropriately assigned to audit teams or to otherwise assist the internal auditors.

Standards of Audit Practice

The Office of Internal Audit will carry out its responsibilities in accordance with University policy, state and federal law, and the ***International Professional Practices Framework.*** The ***Framework*** requires the mandatory adherence to the definition of internal auditing, the ***Code of Ethics*** and the ***International Standards for the Professional Practice of Internal Auditing*** as promulgated by the Institute of Internal Auditors.

_____
Director of Internal Audit

_____
President

_____
Audit Committee Chair

Dated_____

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 11, 2014**

Agenda Item: Consent Report

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

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

Presenters: Gail Klatt, Associate Vice President
Michael Volna, Associate Vice President

Purpose & Key Points

To approve non-audit engagements with external audit firms as follows:

- The University's Health Information Privacy and Compliance Office proposes to engage Deloitte Consulting, LLP to provide advisory services to the University to demonstrate the University's compliance with HIPAA Security requirements and advise the University on areas that may require further analysis and investigation. The fees and expenses for this engagement are estimated to be $293,000.

- The University's Office of the Vice President for University Services proposes engaging Deloitte Consulting, LLP to provide advisory services to the University's Enterprise Asset Management (EAM) project. The EAM project will develop new business processes and systems for maintaining the University's physical plant and infrastructure assets. This engagement is for Phase 1 of the project. Deloitte will provide advice, leading practices, tools, templates, and recommendations to the University for use in designing a leading practice process model, collecting high level functional and reporting requirements, and preparation for selecting and implementing an enterprise EAM solution. The fees and expenses for this engagement are $1,744,000.

The Controller's Office has reviewed the scope, deliverables, and Deloitte's proposed role for these engagements. Engaging Deloitte for this work would not impair the firm's independence with respect to their role as independent external auditor of the University of Minnesota.

Background Information

Approval is sought in compliance with Board of Regents Policy: *Audit Committee Charter*

President's Recommendation

The President recommends approval of these Deloitte consulting engagements.

BOARD OF REGENTS
DOCKET ITEM SUMMARY

Audit **September 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

Emergency Approval of Non-Audit Engagement with External Auditors
On August 5, 2014, Chair Beeson, Vice Chair Johnson, and Audit Committee Chair Brod authorized an emergency approval of an engagement for professional services from an auditing firm as follows:

- The University's Facilities Management (FM) organization requests approval of a consulting services engagement with Deloitte Consulting, LLP, to advise FM on interim planning, and conducting a pilot Business Process Alignment project, in connection with the University's Enterprise Asset Management program. This segment of the program is scheduled for five weeks (August 18 through September 24, 2014). Total fees and expenses are estimated at $244,000.

The University Controller reviewed the proposed scope of services and statement of work, and determined that there would be no impairment of Deloitte's independence with respect to their audits of the University of Minnesota.

The emergency approval was requested because no Board meetings were scheduled for August, and approval was needed to ensure that the related projects proceeded uninterrupted. The approval was consistent with Board of Regents Policy: *Board Operations and Agenda Guidelines*, Section II, Subd. 10, which states:

Upon the recommendation of the president, the Board chair, vice chair, and the respective Committee chair may act on behalf of the Board when delay for Board approval poses a significant health, safety, or financial risk to the University. Any such emergency approvals will be brought to the next meeting of the Board, consistent with Board policy.

Background Information

This information item is presented in conformity with Board of Regents Policy: *Board Operations and Agenda Guidelines*, and is intended to assist the Board of Regents in fulfilling their responsibility for oversight of engagements with external audit firms.