AGENDA


2. The Impact of Sarbanes-Oxley after Six Years: What is Working? - K. Vosen/K. Knudtson (pp. 16-33)

3. Internal Audit Update - G. Klatt (pp. 34-55)

4. Information Items - G. Klatt (pp. 56-57)
Audit Committee

Agenda Item: External Auditor’s Review of Completed Audit Work & Letters to Management

☐ review ☐ review/action ☐ action ☒ discussion

Presenters: Associate Vice President Michael Volna
Kirsten Vosen, Partner, Deloitte & Touche
Tom Roos, Partner, Deloitte & Touche

Purpose:

☐ policy ☐ background/context ☒ oversight ☐ strategic positioning

To update the Audit Committee on the results of the FY 2010 A-133 audit and other audits performed by Deloitte & Touche, and provide an update on the FY 2010 management letter.

Outline of Key Points/Policy Issues:

The A-133 compliance audit is required as a condition of the University receiving federal funding for research, student financial aid, and other federal programs. Deloitte will discuss their audit procedures, conclusions, and reported findings. Deloitte will also communicate their observations on the University’s achievements during the past year, and areas of opportunity for the University.

The management letter communicates the external auditor’s overall observations and findings on internal controls, accounting and reporting, compliance, and other matters. Deloitte has judged that their comments relative to the FY 2010 engagements do not rise to a level of significance that warrants discussion with the Audit Committee, and they will be issuing their letter to University management. Copies of their letter will be made available to the Audit Committee.

Deloitte will also briefly highlight other audit and non-audit engagements performed for the University during FY 2010. All proposed engagements were scrutinized by both Deloitte and the Controller’s Office, and none were judged to impair Deloitte’s independence with respect to performing the University’s annual financial audit.
Background Information:

These engagements are performed annually by the external auditors, and the results are presented to the Board of Regents Audit Committee in conformance with Board of Regents policy: *Board Operations and Agenda Guidelines.*
University of Minnesota
External Auditor’s Review
of Completed Audit Work &
Letters to Management

February 10, 2011
Discussion Topics

• Audit of Federal Programs
  – Compliance Audits
  – University Achievements
  – Opportunities for the University

• Other Communications

• Other University Audits/Procedures
Compliance Audits – Requirements and Communications

• Audit required for federal expenditures in excess of $500,000
  – Total University federal expenditures for 2010 ~$1.034 billion
  – American Recovery and Reinvestment Act (ARRA) expenditures for 2010 ~$83 million
    • $41 million in ARRA expenditures were within the State Fiscal Stabilization cluster (all expenditures were ARRA)
    • $39 million in ARRA expenditures were within the Research and Development cluster

• Identified the following as major award programs to be tested:
  – Research and Development cluster ($456M in 2010 expenditures)
  – Student Financial Aid cluster ($443M in 2010 expenditures)
  – State Fiscal Stabilization cluster ($41M in 2010 expenditures)
  – Cooperative Extension Service ($14M in 2010 expenditures)
  – SNAP cluster ($7M in 2010 expenditures)
  – Education and Human Resources ($4M in 2010 expenditures)
Compliance Audits – Requirements and Communications (cont.)

• Determined testing methodology in accordance with OMB Circular A-133 and OMB Compliance Supplement dated June 2010

• New American Institute of Certified Public Accountants sampling guide required for 2010 - resulted in increased sample sizes

• Additional requirements for ARRA funding
  – Programs that received ARRA funds deemed high-risk
  – Additional work specifically required on ARRA expenditures

• No significant deficiencies or material weaknesses

• Cash management finding – only finding in six major programs tested
Compliance Audits – Requirements and Communications (cont.)

• We audited the University’s compliance with OMB Circular A-133 in accordance with standards applicable to financial audits contained in Government Auditing Standards issued by the Comptroller General of the United States.

• We noted no instances of the following:
  – Significant difficulties encountered in performing the audit
  – Disagreements with management
  – Consultation with other accountants about accounting or auditing matters
  – Major issues discussed with management prior to our retention
  – Fraud, illegal acts, reportable conditions, or material control weaknesses
University Achievements

- Qualification of the University as a low-risk auditee
- No significant deficiencies or material weaknesses in internal control noted
- No material instances of noncompliance for major programs
- Retention of high-quality individuals within Sponsored Financial Reporting as well as the Office of Scholarship and Financial Aid, finance, and accounting departments
- Successful tracking and compliance over ARRA funds
- Student Financial Aid cluster highly automated through use of PeopleSoft
University Achievements (cont.)

• Strong internal audit function with experienced professionals continues to support strong control environment

• Cash management process highly automated and creates short reimbursement lag

• Growth in federal expenditures in the past five years significantly greater than inflation – with $\approx 1B$ of expenditures in fiscal 2010

• Sponsored projects has strong tone at the top
Opportunities for the University

- Create periodic cash reimbursement draw review to help ensure compliance with cash management guidelines

- Continue to assess and monitor state appropriation funding levels in light of the ongoing budget deficit as these funds often support federal program or are used as matching basis for federal dollars

- Continue to utilize full functionality of PeopleSoft to mirror success in Student Financial Aid cluster
Other Communications

Management letter provided to University management regarding the June 30, 2010 audit. We noted no significant deficiencies or material weaknesses requiring a formal communication to the Audit Committee. Full letter available if committee members so desire. A summary of recommendations included:

- Considerations regarding current storage practices for original donor intent documentation to reduce risk of unintended damage
- Periodic write-off of fully depreciated assets to maximize operational efficiency
- Formalize analysis of sponsored revenue transactions that occur subsequent to year-end to ensure appropriate cut-off of revenue recognition
- Investment best practices to formalize management’s consideration and documentation of investment value changes post close through report issuance, management’s determination of GAAP basis fair value adjustment for investments in funds that do not report under GAAP and formalize significant accounting policies and procedures performed by the University in valuing investments and monitor that such policies and procedures are in place
Other University Audits/Procedures

• **Weisman Art Museum**
  – Audit of the Statement of Revenues, Expenses, and Changes in Net Assets

• **Department of Concerts and Lectures**
  – Audit of the Statement of Revenues, Expenses, and Changes in Net Assets
  – Report issued January 10, 2011

• **NCAA Agreed-Upon Procedures**
  – No significant findings

• **Student Fees Agreed-Upon Procedures**
  – Procedures performed for nine student groups

• **Minnesota Job Skills Partnership program**
  – Close-out audit for one program performed in connection with Audit of Federal Programs

• **Minnesota Office of Higher Education**
  – Compliance audit for state grants performed in connection with Audit of Federal Programs
Questions?
As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit and enterprise risk services, and Deloitte Tax LLP, which provides tax services. These entities are separate subsidiaries of Deloitte LLP. Deloitte & Touche LLP will be responsible for the services and the other subsidiaries may act as subcontractors. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.
Audit Committee

February 10, 2011

Agenda Item: The Impact of Sarbanes-Oxley After Six Years: What Is Working?

☐ review  ☐ review/action  ☐ action  ☒ discussion

Presenters: Kirsten Vosen, Partner, Deloitte & Touche
Katie Knudtson, Senior Manager, Deloitte & Touche

Purpose:

☐ policy  ☒ background/context  ☒ oversight  ☐ strategic positioning

The Sarbanes-Oxley Act created new regulatory requirements for publically traded companies, established new expectations for auditors, and set new governance standards for Audit Committees. Through its implementation and over the last six years of its full operation, lessons have been learned as to how to maximize the envisioned benefits and minimize the Acts’ regulatory burden. These lessons are be relevant to the Audit Committee’s theme of “calibrating the University’s risk tolerance in the “new normal” financial environment.”

Outline of Key Points/Policy Issues:

Deloitte and Touche staff will 1) share their experiences in working with organizations subject to Sarbanes-Oxley (SOX), 2) identify practices that have produced the greatest benefits, and 3) discuss the most cost-effective methods for achieving those benefits. The discussion will also highlight changes in the interpretation of the Acts’ requirements that have occurred since its enactment which emphasize the importance of appropriate risk assessment.

Background Information:

Presentations were made to the Audit Committee on the provisions of the Sarbanes-Oxley Act of 2002 and the related implications for the University of Minnesota in November 2002 and February of 2003. The Board of Regents passed the Resolution Relating to Practices Contained in the Sarbanes-Oxley Act of 2002 in May 2003.
University of Minnesota
The Impact of Sarbanes-Oxley After 6 Years: What is Working?

February 10, 2011
Unexpected benefits from Sarbanes-Oxley

*Benefit is to bring operations under better control, standardize fragmented processes, drive down costs, and improve information about the University’s operations*

- Useful to private companies as well as the University of Minnesota
- Unexpected benefits of SOX – Control rationalization
- Ability to pick and choose the SOX practices most relevant to the University without the cost of an opinion
Background

Sarbanes – Oxley Act of 2002 (SOX) – What is it?

• Spotlight on corporate governance

• Demonstration that public companies have effective internal control over financial reporting

• Senior executives are deemed personally responsible for compliance and must attest to the accuracy of their companies’ accounts
  – Identify risks in the organization
  – Identify controls that are in place to mitigate these risks, as well as any control gaps
  – Document both preventative and detective controls
  – RemEDIATE any gaps
  – Verify that controls are working effectively by testing them

• Independent auditor also must provide an opinion on the effectiveness of SOX practices
Background

6 Years Later: Leveraging Auditing Standard No.5 to Streamline SOX Compliance

• Top-down, Risk-based

• AS5’s Impact: Streamlined and less costly SOX compliance

• More flexibility, more discretion, less cost and the ability for smaller public companies to develop their compliance structure

• Focus on entity level controls

• Opportunities for management: Benefits outweigh cost of compliance

• Leverage automated internal controls
COSO: A framework for managing risk

COSO’s Enterprise Risk Management Framework (ERM) was developed in the 1970s, but it remains a valid and frequently used basis for managing risk today, particularly with respect to SOX and Sarbanes-Oxley Rule 404.

- Organize your strategic plan with the COSO Framework – align with strategy, operations, reporting and compliance

- Customize controls according to their most significant risks and complexities
  - Risk tolerance
  - Direct and precise entity level controls
  - Centralized processes and common documentation
  - Leverage information technology and automated controls

COSO’s ERM Framework
Effective risk assessment

An effective risk assessment looks not only at the material financial numbers, but also at the drivers of value and the appetite for risk in the organization.

• Important to view and address risk from an enterprise-wide perspective rather than in silos. Focus on risk you can mitigate

• General practices in managing risk appetite
  – Generally low risk appetite on reputation and regulatory matters
    • Focused on measuring frequency of violations/errors
    • Considerations around establishing tolerance levels
    • Surveys can be used to benchmark and monitor response metrics
  – Measurement and monitoring more qualitative than quantitative
    • Impact
    • Vulnerability
    • Speed of Onset

MARCI Chart – Monitoring Risk Appetite

![MARCI Chart – Monitoring Risk Appetite](image)

- Dot size reflects Speed of Onset
- Low
- Medium
- Med - High
- High

- Assurance / Reassurance of Preparedness
- Enhance Risk Mitigation
- Redeploy Resources
- Measure for Cumulative Impact

Impact of the Risk

Vulnerability
Unexpected benefits of SOX

*Strengthened internal controls and increased leaders’ understanding of strategy, operations, business drivers, and underlying complexities within an organization*

- Enhanced involvement of senior leaders, audit and finance functions, boards, and other oversight committees

- Through the effort of assessing risk, companies have been able to align their resources better with business priorities and key areas of risk – redirect University resources

- Revealed and helped to correct issues in activities such as account reconciliations, approvals, and higher level quality reviews and other critical processes
Unexpected benefits of SOX (continued)

**Strengthened internal controls and increased leaders’ understanding of strategy, operations, business drivers, and underlying complexities within an organization**

- Revealed a variety of inefficiencies, such as multiple ways of entering information into systems and/or duplicate systems that perform the same functions
- Control rationalization: Helped organizations standardize processes, improve quality and consistency, streamline efforts, and cut support costs
- Companies have taken advantage of the automated controls available in their computer systems
- Align resources better with business priorities and key areas of risk
As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit and enterprise risk services, and Deloitte Tax LLP, which provides tax services. These entities are separate subsidiaries of Deloitte LLP. Deloitte & Touche LLP will be responsible for the services and the other subsidiaries may act as subcontractors. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.
Sarbanes-Oxley Act of 2002
Can private businesses benefit from it?
Most executives are familiar with the requirements that the Sarbanes-Oxley Act of 2002 (SOX) imposes on public companies, but SOX practices also may be useful to private companies. Unlike public companies, private company leaders can pick and choose the SOX practices most relevant to their organizations. In fact, many forward-thinking private companies have turned SOX to their advantage — using it not only to preserve value for their stakeholders, but to bring operations under better control, standardize fragmented processes, drive down costs, and improve information about company operations.

Deloitte hosted a Dbriefs webcast on April 22, 2009, to address the unique risks facing private companies and to discuss leading practices for managing risk. More than 1,800 executives joined to learn why private companies might select appropriate SOX practices to protect and grow their businesses, and to share their own views through their answers to polling questions.

Sarbanes-Oxley Act of 2002 (SOX): What is it?
SOX legislation puts the spotlight on corporate governance, making it mandatory for public companies to demonstrate that they have proper financial reporting controls in place. Senior executives are deemed personally responsible for compliance and must attest to the accuracy of their companies’ accounts. An independent auditor also must provide an opinion on the effectiveness of SOX practices. To complete the sign-off, organizations must:

- Identify risks in the organization.
- Identify controls that are in place to mitigate these risks, as well as any control gaps.
- Document both preventative and detective controls and remediate any gaps.
- Verify that controls are working effectively by testing them.

Most of the focus has been placed on internal controls, but SOX legislation also covers areas designed to improve corporate governance and restore trust, such as ethical behavior, board composition, and independence of auditors.

While SOX is required for public companies, you, as the executives, owners, stakeholders, and leaders of private companies have the ability to pick and choose which practices to implement. You can select only the relevant and most helpful elements for the company because this is not all-or-nothing for a private organization.

The unexpected benefits of adopting SOX
The effort involved with implementing SOX has strengthened corporate controls as expected. But, it also has produced some unexpected business benefits for companies that have embraced the legislation — the biggest being enhanced involvement and engagement of senior leaders, audit and finance functions, boards, and other oversight committees. The exercise of applying SOX practices has increased leaders’ understanding of strategy, operations, business drivers, and underlying complexities within the organization. In addition, through the effort of assessing risk, companies have been able to align their resources better with business priorities and key areas of risk. And, the stronger emphasis on controls has revealed and helped to correct issues in activities such as account reconciliations, approvals, and quality reviews and other critical processes.

At the same time, SOX efforts have revealed a variety of inefficiencies, such as multiple ways of entering information into systems and/or duplicate systems that perform the same functions. These findings have helped companies standardize processes, improve quality and consistency, streamline efforts, and cut support costs. Finally, more companies have taken advantage of the automated controls available in their computer application systems to reduce errors and increase efficiency.

Some private company executives may question the benefit of incorporating SOX practices into their businesses because for private companies accountability is private. They may want to keep in mind, however, their long-term plans and the likelihood that the company will transition at some point. Implementing strong governance practices now can help can make it attractive to a new investor or buyer down the road. In addition, establishing governance practices early on may help to ease the assessment process that would be made by a new investor or buyer. Even if future leadership remains with the family, it too can benefit from solid governance practices.
The risks facing private companies

Private companies face a wide array of risks, including economic, operations, insurance, security, business, and process risks. To manage these effectively, it is important to view and address them from an enterprise-wide perspective rather than in silos. In addition, while some risks — such as market risks — are beyond an organization’s control, private companies should focus on the risks they can mitigate. For example, a company can lower its workers compensation insurance risks by understanding the various products available, assessing the measures in place to prevent accidents, establishing processes to resolve claims quickly, and then monitoring data continually to understand where the organization stands.

Private companies’ risks can increase if they lack formal:

- Governance structures and practices to mitigate risk. Many have boards and/or committees, but these often focus on strategy, growth, compensation, and succession rather than risk and controls.
- Risk assessment processes. Private companies can be more likely to rely on trusted individuals rather than processes to protect corporate assets and shareholder value.
- Directions for employees. Reliance on instructions issued by “word of mouth” can lead to inconsistent practices.
- Processes for managing control and reporting problems consistently across locations. In decentralized environments, ad-hoc methods for accomplishing the same task can increase both complexity and cost.
- Internal audit procedures that determine compliance with policies and procedures.

Finally, organizations that have grown substantially over the past several years — as many private companies have — may lack data integrity due to rapid systems changes. This increases the risk of decision-making based on faulty information and/or the cost of improving the information technology (IT) infrastructure to produce quality data.

COSO: a Framework for managing risk

The Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations (the “COSO framework”) is a product of the 1970s’ Treadway Commission, but it remains a valid and frequently used basis for managing risk today, particularly with respect to SOX and Sarbanes-Oxley Rule 404. Many private companies also find it useful for organizing their approach to internal controls because it enables executives to customize controls according to their most significant risks and complexities.

The COSO framework’s horizontal axis incorporates operations, financial reporting, and compliance. While Sarbanes-Oxley Rule 404 deals only with financial reporting, this framework’s broader focus is beneficial in looking at risk across the enterprise. The five elements of the framework — monitoring, information and communications, control activities, risk assessment, and control environment — are areas for private companies to consider in designing their approach to managing risk.

Control environment. The control environment represents the conscience of the organization — the tone from the top. How important is risk management to the organization? Private companies that have established a strong control environment typically have boards that pay attention not only to strategy and growth, but to risk and complexity in the business. These organizations:
• Document company principles and values.
• Establish governance and organizational structures, including the composition of advisory boards, charters, and responsibilities.
• Utilize key performance indicators and dashboards to manage the material numbers and the risks that could impact shareholder value.
• Enhance accountability by requiring that managers attest to their review of certain risk areas, reconciliations, or other data.
• Employ human resources policies and practices that support internal controls and address situations such as conflicts of interest, gifts, and related parties.
• Encourage employees to report situations involving fraud or significant risk.

Many of these tactics are relatively inexpensive to implement, but they can provide benefits in setting the right tone for the organization.

**Risk assessment.** A risk assessment is a quantitative and qualitative approach to evaluating an organization’s significant internal and external issues.

An effective risk assessment looks not only at the material financial numbers, but also at the drivers of value and risk in the organization. It examines elements of the financial statements — both balance sheet and income items — considering factors such as materiality of the account balance, importance to operations, volatility in account balance, subjectivity in determining the account balance, susceptibility to loss or fraud, and the complexity of the calculation. Then, it classifies all elements on a grid based on magnitude of the account and the likelihood of misstatement. A critical final step is reporting the results of the assessment to the board, enabling the company to evaluate and address its significant risks and define a customized approach for addressing them from the top down.

In addition to conducting formal risk assessments, leading private companies may:
• Utilize the risk assessment data to make strategic decisions based on value preservation and value creation rather than risk tolerance.

• Examine and seek to improve the maturity level of the company’s existing control environment.
• Probe the potential impact of risk events.
• Incorporate regulatory requirements into the risk review. For example, companies that accept credit cards must make sure that information is properly obtained, maintained, and purged under Gramm-Leach-Bliley Act (GLBA) rules.

**Control activities.** Control activities are policies and procedures designed to address whether a company has the right controls mitigating the right risks and that those controls are documented and followed. Typical controls include approvals, reconciliations, and segregation of duties. Many organizations only address this area of the model — missing the benefits of a more holistic approach.

Private companies that have implemented effective control activities are likely to:
• Conduct process mapping exercises to match controls to critical business and reporting processes.
• Prepare a gap analysis that guides the development of new controls.
• Issue standard operating procedures that guide the consistency, centralization, and standardization of controls.
• Segregate responsibilities to manage risks of fraud or conflict of interest issues.
Monitor controls to determine whether they mitigate operational, financial reporting, or compliance risks.

Verify that appropriate controls are in place in any new or modified technology.

Leverage the automated control capabilities available in newer systems.

Many organizations have experienced significant growth over the last seven to 10 years. These organizations often find that the process of mapping controls not only aids risk management; it enables them to manage costs by identifying and eliminating redundant activities.

Information and communication. Timely and accurate communication of information helps the organization monitor and understand business and control performance. It also helps employees understand the expectations of them, and provides managers the information they need to avoid surprises and bad decisions. Private companies with effective control-related information and communication practices:

• Provide a confidential mechanism, such as a whistleblower program, to increase their understanding of issues.
• Solicit employee suggestions for improvements or areas requiring attention.
• Reinforce the company’s code of conduct and business ethics through multiple channels.
• Confirm access to reliable and readily available financial and operational reports.
• Protect confidential company and customer information.
• Have business continuity plans in place to protect operations in the event of an outage or disaster.
• Establish clear channels of communications with customers, suppliers, and other third parties — not only to strengthen relationships, but to determine that potential issues are identified, before they become serious.
• Communicate employee duties and responsibilities clearly.

Monitoring. Monitoring processes helps to determine whether internal controls are adequately designed, executed, effective, and adaptive. These activities exist throughout the COSO cube, but positioning this element atop the model can help to substantiate that those activities are actually happening — a model of “trust, but verify.” Employees need to be allowed to carry out their jobs and responsibilities, but they also need to know that someone may check to confirm that they are doing what they are supposed to be doing. At the same time, it is important to make sure that the scope and frequency of monitoring activities are aligned with the significance of risk and the importance of the value driver in question. In other words, measure what matters. Private companies with effective monitoring processes will:

• Build controls — for example, certification — into their normal, recurring operating activities.
• Have an internal audit department or special project resource that can verify control activities and/or assist with addressing specific operational issues.
• Define an escalation path and processes for remediating identified issues.

Getting started with SOX

Although not required for private companies, adopting some SOX principles and practices can be beneficial — not only for risk management, but for performance and shareholder value.

How can you begin to take advantage of SOX? One approach is to start with the end in mind. Applying SOX is a process with many facets. Defining what you want to achieve will help guide your control activities and enable you to focus on the areas that add value to the organization. In addition, employing a top-down approach helps drive attention to important areas of focus and supports proper ongoing reinforcement. Utilizing a sound framework helps organize your activities across a complex environment. Although it is not new, the COSO framework is broadly applicable to both public and private organizations. For private companies, it combines the benefit of organization with the ability to hand pick those elements that will work in your environment — and help you protect and grow your business.
Executives’ views
Deloitte hosted a Dbriefs webcast on April 22, 2009, to address the unique risks facing private companies and to discuss leading practices for managing risk. More than 1,800 executives joined to learn why private companies might adopt SOX practices to protect and grow their businesses and to share their own views through answers to polling questions.

Webcast participants recognized that SOX practices can help private companies grow their businesses while reducing costs. Nearly 38 percent said that private companies will see the greatest impact by strengthening their overall control environment. An almost equal number, 36.2 percent, believed private companies will benefit most by aligning controls properly with the company’s risk assessment. A smaller percentage, 16.6 percent, felt the greatest impact will come from active involvement and engagement from those charged with governance responsibilities. Only 9.6 percent said they believe SOX practices cannot help grow the business or reduce costs.

Although they are not required to implement SOX practices, many private companies do take steps to assess and manage risk at some level. Webcast participants were split with respect to the most prevalent area of risk in their organization. Twenty percent said their most prevalent risk came from informal or ad-hoc processes, nearly 14 percent indicated that it was from data integrity and systems issues, and nine percent responded that it was from a lack of an internal audit function to manage compliance with policies and procedures. Just over a quarter of participants, 27.4 percent, indicated that none of those issues posed evident risks, as their organizations already have adopted several SOX practices. Just over 10 percent said that their

What SOX practice do you believe has the most impact for private companies to help grow the business while reducing costs?

![Pie chart showing responses to the question about the most impactful SOX practice.](chart1.png)

- Strengthening the overall control environment: 37.5%
- Proper alignment of controls with the company risk assessment: 19.3%
- Active involvement and engagement from those charged with governance responsibilities: 16.6%
- None of the above — SOX practices cannot help grow business or reduce costs: 9.0%
- 27.4% indicated that none of those issues posed evident risks, as their organizations already have adopted several SOX practices.

Source: Deloitte’s Private Company Dbriefs webcast, “Sarbanes-Oxley: Can effective practices from public companies benefit private businesses?” held on April 22, 2009. Polling results presented herein are solely the thoughts and opinions of survey participants and are not necessarily representative of the total population of private companies.

What area of risk do you think is most evident in your organization?

![Pie chart showing responses to the question about the most prevalent area of risk.](chart2.png)

- We do not have a formal risk assessment or governance structure in place: 20.0%
- Informal or ad-hoc processes: 13.8%
- Lack of internal audit function to manage compliance with policy and procedures: 10.5%
- Data integrity and systems issues: 9.0%
- None of the above, we’ve already adopted several SOX practices: 9.0%
- Not applicable: 31%
organizations do not have formal risk assessment or governance structures in place.

One of the key steps in managing risk is to perform a detailed risk assessment. More than half of webcast participants, about 56 percent, said their organizations have performed such an assessment, but these respondents are split as to their perceptions on the sufficiency of their internal controls. Just over 30 percent said that while they have performed a detailed risk assessment, more work is needed to strengthen controls, while 25.3 percent felt their controls are adequate. Nearly 14 percent said they have not performed a detailed risk assessment but do need stronger controls. Only about nine percent said that while they have not performed a detailed risk assessment, their current controls are adequate.

Private companies have the opportunity to select from a variety of SOX-related control activities, depending on what is most appropriate for their business. Participants considered several primary control activities and indicated the one most closely aligned with their organizations’ strategies. Nearly half of participants, 47 percent, said that the control activity most aligned to their strategy was “identifying whether existing controls effectively mitigate operational, financial reporting, or compliance risks.” Sixteen percent of participants responded with “automating processes and implementing enabling technology,” and nearly 13 percent responded with “understanding of standard operating procedures for key business processes and IT.” Only seven percent responded with “evaluating responsibilities to avoid fraud and conflict of interest issues.”

Have you performed a detailed risk assessment and feel you have adequate internal controls to address such risk?

- Yes and controls are adequate: 25.3%
- Yes, but more work is needed to strengthen controls: 21.8%
- No, however, controls are adequate: 17.3%
- No and stronger controls are needed: 15.6%
- Don’t know/not applicable: 8.9%
- Don’t know/not applicable: 30.3%

What control activity do you feel is most closely aligned to the strategy of your organization?

- Understanding of standard operating procedures for key business processes and IT: 12.8%
- Evaluating responsibilities to avoid fraud and conflict of interest issues: 17.3%
- Identifying whether existing controls effectively mitigate operational, financial reporting, or compliance risks: 15.6%
- Automating processes and implementing enabling technology: 7.3%
- None of the above/not applicable: 47.0%

About Deloitte Private Enterprise Services

Deloitte’s Private Enterprise Services are designed to assist private companies with their business needs in a holistic manner — ranging from financial and tax reporting for the business to owner wealth management — by drawing on the extensive resources of the Deloitte U.S. firms. Our depth and breadth of experience encompass an array of typical issues for growing enterprises such as business expansion, governance structure, and talent strategies. Our client experiences span various industry sectors and ownership arrangements such as investor-owned, closely held, and family businesses.

Deloitte’s service mission is to build long-term, trusting relationships with our clients. We do this by maintaining a thorough understanding of current issues and long-term goals, listening to our clients, and helping them to make informed and strategically sound decisions. The honesty and integrity of our people and the objectivity of our advice foster our ability to earn and preserve long-term trust and mutual respect.

Learn more about our Private Enterprise Services by visiting our website at www.deloitte.com/us/privateenterprise.
Audit Committee

Agenda Item: Internal Audit Update

Presenters: Associate Vice President Gail Klatt

Purpose:

To update the Audit Committee on Internal Audit activities, results, and observations.

Outline of Key Points/Policy Issues:

• Since our last follow-up for the October 2010 meeting, 43% of the outstanding recommendations rated as “essential” were implemented by University departments. This percentage exceeds our expected implementation rate of 40%. An updated control evaluation chart is included for each audit to show progress made on the “essential” items. Four units fully implemented all their remaining “essential” recommendations.

• Six audit reports containing 10 recommendations rated as “essential” were issued in the last four months.

Background Information:

This report is prepared on a quarterly basis and is presented to the Audit Committee in conformance with Board Operations and Agenda Guidelines.
Internal Audit Update
University of Minnesota Regents Audit Committee
February 10, 2011

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 October 5, 2010

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 “snapshot” 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 2011 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.
Implementation rates were 43% for the period, which exceeds our expected rate of 40%.

Time spent to date on the FY 2011 audit plan is about what was expected and budgeted.

Time spent on investigative activities and special projects is slightly less than what was expected and budgeted for the year to date.
**Status of "Essential" Recommendations as of January 28, 2011**

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Audit</th>
<th># of Essential Recommendations in the Report</th>
<th># of Essential Recommendations Remaining From Prior Quarter</th>
<th>Current Quarter Results</th>
<th>Overall Progress Towards Implementation*</th>
<th>Any Individual Issues With &lt; Satisfactory Progress?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug-07</td>
<td>UM - Morris Campus</td>
<td>12</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Aug-08</td>
<td>AudienceView Ticketing System</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Sep-08</td>
<td>Department of Mechanical Engineering</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Mar-09</td>
<td>Department of Concerts &amp; Lectures</td>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Mar-09</td>
<td>Center for Magnetic Resonance Research</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>Completed</td>
</tr>
<tr>
<td>Jun-09</td>
<td>Sponsored Project Sub-Awards</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Jul-09</td>
<td>OIT Database Administration</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Jul-09</td>
<td>Effort Certification</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Aug-09</td>
<td>School of Dentistry</td>
<td>11</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Oct-09</td>
<td>Academic Health Center Information Systems</td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Dec-09</td>
<td>Payment Card Industry Compliance</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Dec-09</td>
<td>Depts of Med., Dermatology &amp; Their Admin. Service Ctr.</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Jan-10</td>
<td>Google Applications for UMN</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Jan-10</td>
<td>Office of Student Finance</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td>Completed</td>
</tr>
<tr>
<td>Jan-10</td>
<td>UM - Crookston Campus</td>
<td>14</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Jan-10</td>
<td>Non-Sponsored Accounts Receivable</td>
<td>10</td>
<td>7</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Apr-10</td>
<td>Job Scheduling - EFS</td>
<td>6</td>
<td>5</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Jun-10</td>
<td>University Services IT</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Sep-10</td>
<td>Upward Bound</td>
<td>16</td>
<td>16</td>
<td>12</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Sep-10</td>
<td>OIT Change Control</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Sep-10</td>
<td>UMD Facilities Management</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>Completed</td>
</tr>
<tr>
<td>Sep-10</td>
<td>CFANS Research and Outreach Centers &amp; Cloquet Forestry Center</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Total: 143 82 35 40 7

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

- **Morris has made significant progress in resolving a number of old outstanding audit issues. In addition to taking action to justify marking 50% of the issues as implemented, Morris has made changes on the remaining issues so their risk profile associated with each finding is reduced.**

**"Essential" Recommendation Implementation Trends**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># of Essential Recommendations Receiving Follow-up</td>
<td>82</td>
<td>80</td>
<td>103</td>
<td>101</td>
<td>108</td>
<td>132</td>
<td>179</td>
<td>144</td>
<td>157</td>
</tr>
<tr>
<td># of Recommendations Considered Fully Implemented</td>
<td>35</td>
<td>27</td>
<td>30</td>
<td>47</td>
<td>39</td>
<td>44</td>
<td>53</td>
<td>57</td>
<td>35</td>
</tr>
<tr>
<td>Implementation Percentage</td>
<td>43%</td>
<td>34%</td>
<td>29%</td>
<td>47%</td>
<td>36%</td>
<td>33%</td>
<td>30%</td>
<td>40%</td>
<td>22%</td>
</tr>
<tr>
<td>Audit/ Report Date</td>
<td>Status-Partially Implemented (P) or Not Implemented (N)</td>
<td>Senior Management Contact</td>
<td>Summary of the Issue/Risk Involved</td>
<td>Current Comments From Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University of Minnesota - Morris Aug-07</td>
<td>P</td>
<td>Lowell Rasmussen Jacqueline Johnson</td>
<td>UMM should develop a formal process for managing system changes so management can be assured only tested and authorized changes are moved into production. Test environments should be established. The process for making changes to production should be modified to ensure: • the implementation plan is well thought out and documented; • roll back strategies/plans are defined and documented; • no changes are moved into production without formal testing; • test plans and results are documented and retained; • peer and/or management review occurs before the change is implemented; and • no changes are moved into production without a record demonstrating IT management and application owner approval.</td>
<td>Morris has significantly reduced this risk by moving most critical applications to the Twin Cities. The Bursar application, Compass, and Bookstores application have already transitioned to the Twin Cities. The Housing application is the only critical application still managed at Morris. Computing Services has implemented a change tracking process for network, system, and application changes. This process aligns with OIT’s change control practices. Alignment activities occurring in Spring/Summer 2011 are expected to resolve the rest of this finding.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>Lowell Rasmussen Jacqueline Johnson</td>
<td>The network design of UMM should be reconfigured to ensure that no single point of failure exists for any critical business processes. Management should continue developing procedures for enforcing consistency in device settings and should consider deploying an automated tool to manage network device configurations. Any variances in configuration settings should be documented (i.e., the need for the variance should be explained).</td>
<td>Computing Services is working with OIT to assist with a network upgrade. Plans are being developed that will transition Morris network management activities to OIT, and re-position Computing Services staff into a local on-site hardware support role (installation, replacement, etc). This project is moving forward, with work expected to begin in Summer 2011.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>Lowell Rasmussen Jacqueline Johnson</td>
<td>UMM Computing Services should ensure that all production systems are adequately backed up, backup files are moved offsite, and that the backups are systematically tested. Senior management should develop a plan to ensure that staffing is adequate to continue business operations in the event of a disaster. UMM Computing Services should also ensure that equipment is available to continue business operations in the event of a disaster. UMM Computing Services, in collaboration with senior UMM management, should ensure that Disaster Recovery plans are completed and tested. Steps should be taken to ensure the Disaster Recovery plans include: • expectations in the event of a disaster, • roles and responsibilities, • resources needed to recover the system, • procedures for activation of the plan and escalation processes, • priorities for system restoration, • contact information for recovery team members, • test plans for ensuring the system is functioning as intended and the integrity of data was not compromised, and • the time interval for regular testing of the disaster recovery plan. In addition, management should ensure that the disaster recovery team is trained in their responsibilities in the event of an emergency and are aware of manual or alternate processing procedures that are to be used when processing is delayed for an extended period of time.</td>
<td>The Campus IT Director has implemented changes that significantly reduce the risk to the campus in the event of an outage. Additional changes are already in process. Critical web sites are currently being migrated to OIT servers, which will further reduce risks to the campus. Computing Services has completed phase 1 of its disaster recovery plan (identify applications, owners, criticality, dependencies, usage, etc). Phase 2 will begin in Spring/Summer 2011, after servers migrate to OIT, to reduce the scope of the remaining disaster recovery planning effort.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# of Items 3
<table>
<thead>
<tr>
<th>Audit/Report Date</th>
<th>Status—Partially Implemented (P) or Not Implemented (N)</th>
<th>Senior Management Contact</th>
<th>Summary of the Issue/Risk Involved</th>
<th>Current Comments From Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Ticketing System (AudienceView)</td>
<td>P</td>
<td>Liz Eull, Steve Rosenstone</td>
<td>Access to the AudienceView application should be granted through Central Authentication Services using x.500 usernames and passwords. Privileged user access to the AudienceView application, database or server should require M Key token and pin authentication. No account username or password should ever be shared by more than one individual in the application, database or on the server. This is especially true for privileged accounts and service accounts used for process automation. Audit trails at the AudienceView application; database and server level should be secured and monitored. As OIT has identified a product for performing this function at the server level, they should move quickly toward implementing the solution. Access rights assignments should be reviewed on a periodic basis by appropriate managers. Records of rights assignment authorization should be retained for the life of the access authorization. Records of the periodic review should be maintained for a reasonable period (e.g., one year). Documentation of access assignment processes and security methodologies should be maintained at each level of the AudienceView system. System interfaces and design should be documented and tested for assurance that all interfaces to and from the system are secure. An automated interface to the general ledger system, EFS, should be considered for greater control of this process. Reconciliation processes should be immediately redesigned to comply with University policies and procedures and thoroughly documented. The goal should be that the process should ensure that transactions are not being lost, duplicated or corrupted. Key edits and controls, (like pricing limits and duplicate customer elimination), should be identified by OIT and Athletics management and implemented to mitigate the risk of inaccurate data in the AudienceView system. The additional edits should include supplemental edits preventing future duplicate customer entries. Current duplicate customers in the system should be identified and removed from the system. Athletics and OIT support staff should work together to prioritize a list of defects and desired enhancements to the system. Athletics should document all of their business processes around and through the AudienceView system with the assistance of OIT staff. Clear expectations should be established by both OIT and Athletics to ensure effective progress towards University goals, and to ensure that the University can reap the most benefits from the AudienceView system while providing University customers a professional, reliable, and easy to use ticketing system.</td>
<td>Athletics and Concerts and Lectures management believe recent changes to address some of the access control issues outlined in this finding have significantly reduced the control concerns. Those actions have resulted in:  - All employees now having their own login and passwords, so passwords are not shared and all accounts can be tied to individual users,  - All terminated employees having their login credentials deleted from the AudienceView application immediately, and  - Access privileges being reviewed after both Northrop/Arts and Athletics made the change to a hosted solution. Going forward all access rights will be reviewed once a year or if there is a change in job responsibilities.</td>
</tr>
<tr>
<td>Audit/ Report Date</td>
<td>Status-Partially Implemented (P) or Not Implemented (N)</td>
<td>Senior Management Contact</td>
<td>Summary of the Issue/Risk Involved</td>
<td>Current Comments From Management</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Department of Mechanical Engineering</td>
<td>P</td>
<td>Sue Mantell Uwe Kortshagen</td>
<td>An efficient and effective process should be implemented to verify that all workstations used by department staff are configured to satisfy the security standards established by OIT (i.e., the equipment should be configured to pass the quick start tests). Management should develop a formal inventory of all computer equipment owned/used by its personnel. Once that inventory is developed, management should develop a plan to transition system support for all computers used by ME to its central IS staff or implement a process to ensure that security risks are formally evaluated and properly managed. A process should be established to communicate security standards and expected behavior by ME staff, including quick involvement by management when security standards are circumvented by individual staff actions.</td>
<td>Mechanical Engineering is on track to implement active directory on the majority of our computers by the July 31st deadline. For the remaining computers, Mechanical Engineering is developing an exemption process with assistance of the college's IT representative to the institution's IT Leadership Alliance.</td>
</tr>
</tbody>
</table>

| # of Items | 1 |
| **Total:** | 6 |
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 September 2010, 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
Department of Mechanical Engineering (September 2008)

Current Quarter Evaluation

Department of Concerts & Lectures (March 2009)
Original Report Evaluation

Previous Quarter Evaluation

Current Quarter Evaluation

University Services IT (June 2010)

Upward Bound (September 2010)
Units with Charts that Fully Implemented their "Essential" Recommendations During the Past Quarter

Original Report Evaluation

Previous Quarter Evaluation

Current Quarter Evaluation

Center for Magnetic Resonance Research (March 2009)

Departments of Medicine, Dermatology & Their Administrative Service Center (December 2009)

Department of Medicine

Adequate Control

Significant Control Level

Critical Control Level

Potential Over-Control
Audit Activity Report

Scheduled Audits

- Completed audits of: Veterinary Diagnostic Labs, UMD University Relations, a review of small dollar vendor payment transactions, OIT Data Network, the University Procurement Card Program, and a review of the UMD Chancellor & Vice Chancellor Offices and expenses. Details are shown on the following charts.

- Began/continued audits of: Sponsored Financial Reporting, Boynton Health Service, the Office of Real Estate Management, CLA IT management, a review of the President and Vice President Offices and expenses, Eastcliff, the Department of Civil Engineering, UMD Athletics, University Payroll, Intercollegiate Athletics NCAA Compliance, Admissions, and the OIT Data Center.

Investigations

- Performed investigative work on 13 issues in accordance with the University Policy on Reporting and Addressing Concerns of Misconduct.

Special Projects

- Provided consulting services related to: data security, equipment disposal, controls associated with the AudienceView ticketing system, Google HIPAA compliance, data center management and consolidation efforts, software as service standard, the In Common Silver federation project, identity management tool RFI project, building access monitoring, information technology concerns associated with building system automation controls operations, and University payroll exception testing.

Other Audit Activities

- Participated in the following:
  - HRMS PeopleSoft Steering Committee
  - Fairview Health Systems Audit Committee
  - University of Minnesota Foundation Audit Committee
  - Executive Compliance Oversight Committee
  - Institutional Conflict of Interest Committee
  - IT Leadership Alliance
  - OSH Steering Committee
  - President’s Policy Committee
  - Board of Regents Policy Committee
  - President’s Advancing Excellence Committee
  - Risk Tolerance Work Group
  - Office of Human Resources Cost of Selection Committee
  - Institutional Conflict of Interest Policy Review Committee
We believe VDL has developed a control environment and a system of internal control that addresses most major business and compliance risks. Opportunities for improvement were identified in the areas of account receivable monitoring and information system controls.

The mission of the Office of Vice Chancellor of University Relations is “to provide information, services, and giving opportunities which support the University while fostering a relationship of goodwill and understanding with UMD alumni, the community and beyond.” We believe University Relations has developed a control environment and a system of internal control that addresses most major business and compliance risks. Both the nature and the number of issues in this report reflect a strong control environment; especially since this was our first audit of UMD University Relations.
Controller's Office: Voucher Transactions <$100

Due to the limited scope and system-wide nature of this audit a control evaluation chart was not developed for this report.

This audit was planned in response to the implementation of the new Enterprise Financial System (EFS) and the functionality of "auto approval" within the system for voucher transactions less than $100. This functionality allows certain small dollar payments to vendors to be entered to EFS and be paid without an electronic approval. The audit focused on both compliance with University purchasing policies and testing to determine whether there was evidence of inappropriate purchases, including payments for goods or services that might be personal in nature. We believe departmental adherence to policy regarding processing of voucher transactions under $100 is generally good. While it is difficult to detect all possibilities of fraudulent activity, none of the sample transactions tested provided any indication of improper actions.

OIT NTS

This audit focused on the University's data network provided by OIT's Networking & Telecommunications Services (NTS) known as the Gopher GigaNet. The University data network is well designed and well managed. The necessary resources are in place and available to address current and future demands. Network redundancy is in place to support resiliency. Substantial security measures have been deployed to ensure integrity and reliability. Areas requiring some management attention include physical, logical, and remote access.
Disbursement Services has developed a control environment and a system of internal control that addresses most of the business and compliance risks associated with operation of the PCard program. While acknowledging the inherent risks of fraud in small dollar purchasing activities such as this, control systems have remained strong to address the risks of the program. Several areas that were not addressed immediately following the EFS implementation have been improved and are better managed, including becoming more current on missing imaged reports through better enforcement and more timely card deactivation for non-compliers. Controls do need to be improved over the manual approval process used for transactions that do not receive electronic approvals in EFS.

As the chief administrative officers at UMD, the Chancellor's and Vice Chancellors' Offices are expected to set the standard of accountability for the entire campus. Based on the results of our audit, we feel they have been successful in meeting that responsibility.
Audit Committee

February 10, 2011

Agenda Item: Information Items

☐ review  ☐ review/action  ☐ action  ☒ discussion

Presenters: Associate Vice President Gail Klatt

Purpose:

☐ policy  ☐ background/context  ☒ oversight  ☐ strategic positioning

To report engagements with auditing firms that do not require prior approval by the Board.

Outline of Key Points/Policy Issues:

In addition to the annual audit and non-audit services performed by Deloitte & Touche, LLP, which they will be reporting on as part of their February, 2011 update to the Audit Committee, the following engagements are being reported to the Audit Committee:

- The University Tax Department has engaged Deloitte to provide tax consulting services in connection with filing a group exemption application for the Minnesota 4-H Clubs and Affiliated 4-H organizations. Deloitte is providing $15,000 worth of professional services on a pro bono basis for this engagement.

- The University of Minnesota - Duluth entered into an agreement with Licari Larsen & Co, LTD to provide an audit of the financial statements of radio station KUMD as of June 30, 2010. 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 $4,900.

- The Tweed Museum of Art at the University of Minnesota - Duluth entered into an engagement with Charles Zeigler to prepare a statement of financial activity for the fiscal year 2010 to be used as financial support for grant applications. The fees for this engagement are not to exceed $1,600.

The above engagements were reviewed by the Controller’s Office, and none were determined to impair the independence of the accounting firms that were engaged, as related to an external audit of the University. They were approved by the Controller’s Office in conformance with Board Policy.
Background Information:

The Board of Regents reserves to itself authority to approve the selection and engagement of external public accountants by Board of Regents Policy: *Audit Committee Charter*. Engagements for audit and non-audit services with any independent auditor that do not exceed $25,000 and that do not impair the independence of the firm may be approved by the Controller. The engagements must then be reported to the Audit Committee at the next Audit Committee meeting.