UNIVERSITY OF MINNESOTA

BOARD OF REGENTS

Audit Committee

Thursday, October 7, 2010

8:45 - 9:45 a.m.

600 McNamara Alumni Center, East Committee Room

Committee Members
Steven Hunter, Chair
Linda Cohen, Vice Chair
Richard Beeson
John Frobenius
Maureen Ramirez
Patricia Simmons

Student Representatives
Matt McGechy
Matt Privratsky

AGENDA

1. Committee 2010-11 Workplan - S. Hunter/G. Klatt (pp. 2-3)

2. External Audit Update - M. Volna/K. Vosen/K. Knudtson (pp. 4-6)

3. Internal Audit Update - G. Klatt (pp. 7-34)

4. Information Items - G. Klatt (p. 35-36)
Audit Committee

October 7, 2010

Agenda Item: Committee 2010-11 Workplan

☐ review  ☐ review/action  ☐ action  ☑ discussion

Presenters: Regent Steven Hunter
Gail Klatt, Associate Vice President

Purpose:

☐ policy  ☐ background/context  ☑ oversight  ☐ strategic positioning

The purpose of this discussion is to finalize the committee workplan for the upcoming year.

Outline of Key Points/Policy Issues:

The 2010-11 Audit Committee workplan continues the theme of: **Calibrating the University’s risk tolerance in the “new normal” current economic environment.**

The thematic discussions included in the workplan focus on the oversight and monitoring of risks in areas of the University which are critical to the achievement of the University’s goal to become one of the top three research universities in the world. The included topical discussion items are also highly relevant to the Audit Committee’s institutional risk assessment.

The workplan also ensures the Committee receives the information necessary to carry out the governance responsibilities assigned to it in its Charter, including the supervision of the external auditor and oversight of the internal audit program. It also ensures that the Audit Committee is well informed regarding the institutional compliance program.

Background Information:

Each standing committee of the Board of Regents establishes an annual workplan. The workplan is a means to assist the Committee in discharging its responsibilities under its Charter and provides a structure to ensure the topics of highest priority receive the Committee’s attention.
**Board of Regents Audit Committee**  
*2011 Work Plan*  

<table>
<thead>
<tr>
<th>Work Plan Theme:</th>
<th>“Calibrating the University’s risk tolerance in the ‘new normal’ financial environment”</th>
</tr>
</thead>
</table>
| October:         | Audit Committee Workplan (S. Hunter)  
|                  | External Audit Update (Deloitte)  
|                  | Internal Audit Update (G. Klatt)  
|                  | Even though the committee will meet in October, it will also 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. |
| November:        | External Auditor Report (Deloitte)  
|                  | Compliance Officer Report (L. Zentner)  
|                  | **Risk Tolerance Discussion Update (Mulcahy)**  
|                  | Information Item: Semi Annual Controller’s report  
| February:        | External Auditor’s Review of Completed Audit Work and Letters to Management (Deloitte)  
|                  | **The Impact of Sarbanes-Oxley after six years; what’s worked (Deloitte)**  
|                  | Internal Audit Update (G. Klatt)  
| March:           | External Auditor Review (Fees and 2012 Engagement) (M. Volna)  
|                  | **Conflict of Interest and Conflict of Commitment (Zentner and Sullivan)**  
|                  | **Emerging Issues in Higher Education and Audit Committee Impact (DeHaas, Deloitte)**  
|                  | Information Item: External Auditor Relationships and Services Provided  
| May              | External Audit Plan (Deloitte)  
|                  | Compliance Officer Report (L. Zentner)  
|                  | **The University’s Assurance Map – Where is Monitoring Occurring (Zentner, Klatt)**  
|                  | Internal Audit Update (G. Klatt)  
|                  | Information Item: Semi-Annual Controller’s Report  
| July             | Internal Audit Plan (G. Klatt)  


Audit Committee

October 7, 2010

Agenda Item: External Audit Update

☐ review ☐ review/action ☐ action ☑ discussion

Presenters: Associate Vice President Michael Volna
Kirsten Vosen, Partner, Deloitte & Touche LLP
Katie Knudtson, Senior Manager, Deloitte & Touche LLP

Purpose:

☐ policy ☑ background/context ☐ oversight ☐ strategic positioning

To provide the Audit Committee with a status report on the FY 2010 annual audits.

Outline of Key Points/Policy Issues:

Deloitte will update the Committee on its progress with the June 30, 2010 annual external audits, which are currently underway. The University Controller will present the timeline for Committee members’ review of the FY 2010 draft annual financial report.

Background Information:

The External Audit Plan was presented to the Audit Committee at the June 2010 meeting.
External audit update

Financial statement audit

• RUMINCO

NCAA agreed-upon procedures

Compliance audits

• OMB Circular A-133

• MOHE

• Close-out audits

Consistent with past practice, the Board of Regents Audit Committee members will have an opportunity to review a draft of the University’s fiscal year 2010 annual financial report before Deloitte and Touche, the University’s external auditors, sign off and issue their opinion. This review process emanates from the Sarbanes-Oxley Act of 2002 (“SOX”). Although SOX does not apply to the University as a matter of law, the Audit Committee adopted a number of SOX provisions as best practices, including this review process.

The tentative timeline for the review process is as follows:

**Friday, October 22, 2010** – Draft of June 30, 2010 financial report will be delivered to Audit Committee members.

**Sunday, October 24 - Wednesday, Oct. 27** – Committee members review draft report, and communicate any questions or concerns to Audit Committee chair.

**Thursday, October 28, 2010** – Call with Audit Committee Chair and Controller to communicate any comments from Committee members, and obtain approval to issue report.

**End of day, October 28** – Planned date for external auditor signoff on final report.

We anticipate that any changes to this timeline resulting from final audit work would be minor, and will be discussed with the Chair of the Audit Committee in advance.
Audit Committee

October 7, 2010

Agenda Item: Internal Audit Update

☐ review  ☐ review/action  ☐ action  ☑ discussion

Presenters: Associate Vice President Gail Klatt

Purpose:

☐ policy  ☑ background/context  ☑ oversight  ☐ strategic positioning

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 June 2010 meeting, 34% of the outstanding recommendations rated as “essential” were implemented by University departments. This percentage is close to our expected implementation rate of 40%. An updated control evaluation chart is included for each audit to show progress made on the “essential” items. Five units fully implemented all their remaining “essential” recommendations.

• Eight audit reports containing 29 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.
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 1, 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.
Update on the Status of Special Projects, Investigations, and Carryover Audits

- Since our last update in June we have made substantial progress towards completion of many projects that were in process at that time. Work on several major special projects and investigations has been completed, and no new major projects of this type have required our involvement. In addition, 6 of 12 scheduled audits that were carried over from FY 2010 have since been fully completed and issued, and significant progress has been made on the others since July 1.
## Status of "Essential" Recommendations as of September 24, 2010

<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 Implemented</th>
<th>Partially Implemented</th>
<th>Not Implemented</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>
<td>(A)</td>
<td></td>
</tr>
<tr>
<td>Jan-08</td>
<td>College of Biological Sciences</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Jul-08</td>
<td>College of Food, Agricultural, &amp; Natural Resource Sciences</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Aug-08</td>
<td>AudienceView Ticketing System</td>
<td>7</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Sep-08</td>
<td>Review of Capital &amp; HEAPR Proj. Funded by '06 State Debt</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Sep-08</td>
<td>Department of Mechanical Engineering</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jan-09</td>
<td>OIT Security &amp; Assurance</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>Completed</td>
<td></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></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Mar-09</td>
<td>Center for Magnetic Resonance Research</td>
<td>4</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jun-09</td>
<td>Sponsored Project Sub-Awards</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jul-09</td>
<td>OIT Database Administration</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jul-09</td>
<td>Effort Certification</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Aug-09</td>
<td>School of Dentistry</td>
<td>11</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Oct-09</td>
<td>Academic Health Center Information Systems</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Dec-09</td>
<td>Payment Card Industry Compliance</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Dec-09</td>
<td>Departments of Medicine, Dermatology &amp; Their Admin, Service Center</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jan-10</td>
<td>Google Applications for UMN</td>
<td>3</td>
<td>2</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jan-10</td>
<td>Office of Student Finance</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jan-10</td>
<td>UM - Crookston Campus</td>
<td>14</td>
<td>10</td>
<td>1</td>
<td>9</td>
<td></td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Jan-10</td>
<td>Non-Sponsored Accounts Receivable</td>
<td>10</td>
<td>10</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>Satisfactory</td>
<td></td>
</tr>
<tr>
<td>Mar-10</td>
<td>UMD Labovitz School of Business &amp; Economics</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Apr-10</td>
<td>Job Scheduling - EFS</td>
<td>8</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>Satisfactory</td>
<td></td>
</tr>
</tbody>
</table>

**Total:** 136 80 27 42 11

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

(A) Morris has recently hired a new IT director. The IT director has developed plans to address all of the outstanding issues identified in this audit. While none of the findings have been resolved, Morris is now making material progress in improving its overall IT risk profile.

### "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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># of Essential Recommendations Receiving Follow-Up</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>
<td>102</td>
<td>123</td>
</tr>
<tr>
<td># of Recommendations Considered Fully Implemented</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>
<td>31</td>
<td>40</td>
</tr>
<tr>
<td>Implementation Percentage</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>
<td>30%</td>
<td>33%</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>
<td></td>
</tr>
<tr>
<td>------------------</td>
<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>Procedures should be established to immediately evaluate the configuration of all servers for compliance with OIT security standards. Once the evaluation is completed, steps should be taken to quickly make necessary modifications to bring the equipment into compliance or take the equipment out of service. Plans to eliminate or upgrade servers with unsupported operating systems should be completed. Management should continue with its plans to consolidate applications on servers that establish VM environments so consistent configuration, that comply with OIT security standards, can be implemented more quickly. The analysis and corrective action should include servers hosting sensitive data which are not housed in the UMM Computing Services data center (e.g., the Bookstore server). To ensure workstations are configured in a consistent and secure manner which complies with OIT standards, UMM Computing Services should move forward with its plans to begin implementing Active Directory services on staff and faculty workstations. Formal processes should be implemented to ensure UMM Computing Services is notified whenever computer equipment is acquired or disposed. For the purpose of prioritizing security configuration improvements, UMM Computing Services should take steps to identify workstations which process sensitive data or are used to perform critical business functions (e.g., workstations in the Bursar and Bookstore operations). Workstations which process sensitive data, or are used to perform critical business functions, should be immediately reconfigured to comply with OIT Securing Private Data standards and then assigned a high priority in the process of conversion to Active Directory. During the interim prior to conversion to Active Directory, UMM Computing Services may want to use the level 2 QuickStart tool to help evaluate compliance. Steps should also be taken to ensure all laptops are secured with cable locks and data file encryption is enabled. Formal procedures should be established for securing and monitoring system logs. The monitoring process should be performed on a regular basis for all servers and network equipment. Consideration should be given to automating the analysis of the logs and reporting suspicious trends</td>
<td>Jim Hall, new Campus IT Director, has written a System Standards document for Morris Computing Services. This System Standards document is strongly aligned with OIT Standards and Guidelines, and includes new procedures that will be implemented before the end of the calendar year (2010). This is expected to resolve most of this finding.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>Lowell Rasmussen</td>
<td>to technical support staff on a real time basis. Procedures should include establishing requirements that suspicious activity trends are documented. UMM Computing Services should also develop formal/documentated strategies and protocols for dealing with potential incidents such as server compromises, stolen computers, and break-ins where computer equipment is located. The strategies and protocols should leverage processes already established by OIT Data Security and Assurance.</td>
<td>Computing Services improved the physical security over the summer to significantly reduce risks identified in the 2007 audit. Planning is currently underway with Plant Services and Campus Security to add physical security improvements in FY11. This work is expected to be completed in Spring 2011.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jacqueline Johnson</td>
<td>Servers hosting sensitive or mission critical applications and key network equipment should only be housed in a physically secure data center/equipment room which has mechanisms in place to ensure: • unauthorized access is prevented (i.e., door locks for the UMM Computing Services space should be changed to regain control of who has keys, policies should be established and enforced against propping open data center doors, and windows should be eliminated or constructed of attack resistant material); • access to the data center and network equipment room is limited to only those individuals who have a business need; • a card key access system is installed to establish effective access logging; • access rights and access logs are periodically evaluated; • fire detection and suppression mechanisms are in place in all spaces containing key equipment; • all servers and key network equipment is protected by UPS systems with procedures in place to notify UMM Computing Services staff in a timely manner if the UPS is activated; and • effective action plans are in place for notification of UMM Computing Services staff regarding significant rise in temperature that could adversely affect computing systems located in the data center/equipment room. In addition, UMM Computing Services and Plant Services should move forward with their plans to install the recently ordered locking metal cabinets for networking equipment in wiring closets. The cabinets should reduce the risk of tampering and help protect the equipment from environmental and chemical damage.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| N                  | Lowell Rasmussen                                        | Jacqueline Johnson        | 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. | Computing Services is implementing a change control process for network and system changes that will align with the institution's technology change-management program and best practices. This will be in place in Fall 2010. |
| N                  | Lowell Rasmussen                                        | Jacqueline Johnson        | 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). | Computing Services is working with the University's Office of Information Technology to assist with a network upgrade. Plans are being developed that will transition core Morris network management activities to OIT and re-positioning UMM Computing Services staff as the local on-site support (installation, replacement, etc.) role. |
| N                  | Lowell Rasmussen                                        | Jacqueline Johnson        | Management should secure and monitor the audit trail as indicated in finding #2. Management should also develop a written system administration manual with procedures to effectively manage and monitor privileged access including:  
• a formal process for granting, revoking, and modifying privileged access and enforcing periodic password changes for privileged user IDs,  
• a process to ensure that system administrators first sign in using a personal user ID not as root,  
• establishing password protection for server consoles in the data center, and  
• creating a policy disallowing the use of the server consoles to perform day-to-day system administrator functions. | The System Standards document referred to in Finding 2 (above) will resolve this issue. |
<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>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.</td>
<td>Changes have recently been implemented by the new Campus IT Director that reduce the risk to the campus in the event of an outage. Additional improvements will come with the disaster recovery plan, and in realigning the IT support model at Morris. Computing Services plans to complete Phase 1 of its disaster recovery plan (identify all applications, owners, criticality, dependencies, usage, etc) in mid-October. The results of this phase will inform the actual plan – which is expected to include better redundancy, so that the risks of a campus-wide failure from a single outage are significantly reduced.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• expectations in the event of a disaster,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• roles and responsibilities,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• resources needed to recover the system,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• procedures for activation of the plan and escalation processes,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• priorities for system restoration,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• contact information for recovery team members,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• test plans for ensuring the system is functioning as intended and the integrity of data was not compromised, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the time interval for regular testing of the disaster recovery plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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></td>
<td></td>
</tr>
<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;</td>
<td>Central Authentication was suggested and we are reviewing this at this time. Since we have gone to a hosted solution we are reevaluating the risks involved. We have in place a 3-step authentication process for our ticket office staff at this time for work that takes place in our ticket offices. They have to gain entrance into the ticket office, they have to login into active directory with their x500 and then login into AudienceView. The area still under evaluation is remote access. We will be evaluating the methods of access over the next 4 months and work with OIT to establish a plan for remote access.</td>
</tr>
<tr>
<td>Aug-08</td>
<td></td>
<td></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Documentation of access assignment processes and security methodologies should be maintained at each level of the AudienceView system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>Liz Eull</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steve Rosenstone</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>With the move to version 5.0.2 of AudienceView from version 4.1.2 - new functionality is now available. We are working with AudienceView to create better interfaces with other applications on the reporting side of the system. A new automated method has been and is being tested for donations so they will go directly into the DMS system on a daily basis. This should be in place in the next 4 months.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We will be investigating new functionality and reports to determine what other processes can be automated. This investigation will take place over the next 6 months.</td>
<td></td>
</tr>
</tbody>
</table>

# of Items 2
<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>Department of Mechanical Engineering Sep-08 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. ME is aware that the University of Minnesota has adopted a new policy towards workstation security which includes a requirement that University owned desktop and laptop computers be compatible with the Active Directory Architecture. The Mechanical Engineering Department will comply with this requirement. Our current inventory of desktops/laptops includes machines that are managed by our IT staff (enet staff) and unmanaged machines (in which the primary user retains administrative privileges). Within this group of unmanaged machines there is a subset that is used in instructional labs, research labs and machining equipment within the research shop. This subset includes machines that have unique software or hardware requirements that are not compatible with Active Directory. Thus, we have three categories of workstations within the department: (1) managed machines, (2) unmanaged machines serving unique laboratory requirements and (3) unmanaged machines. The current status on moving to the Active Directory Architecture is as follows for each category. For managed machines, we will convert all managed machines to the Active Directory architecture by July 2011. As part of this conversion, we have installed two trial cases in our department. We currently have one server running on active directory that services our research shop (serving 8 staff members). We have rebuilt a typical workstation to run Active Directory. These activities were completed during the summer (2010) and have allowed our IT staff a chance to access the feasibility of switching all managed machines to Active Directory by July 2011. All computers purchased after November 1, 2010 will be managed by department IT staff. Thus, new computer purchases will be converted as part of the conversion of managed machines. For unmanaged machines that have unique software and hardware requirements, we will work with OIT security and assurance to develop an exemption process. It is anticipated that the exemption process will include criteria to define computers that fit into this category. Our computing committee will meet with personnel from OIT by December 1, 2010 to establish the criteria for exemption. Existing unmanaged machines will be required to convert to Active Directory by the date set by the University guidelines, July 1, 2011. As part of the plan to convert all non-exempt computers to Active Directory, we have included an agenda item on our upcoming faculty meeting (October 1, 2010) to discuss the departmental computer policy. Substantial enhancements were made to the draft Disaster Recovery plan over the last quarter. The plan was reviewed by the University Disaster Recovery Coordinator. Mechanical Engineering has addressed some of the improvements suggested by the Coordinator but there are others that still need further action. This finding will be completed once the plan has been appropriately expanded and tested.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

P | Sue Mantell Uwe Kortshagen | ME should develop a formal Disaster Recovery Plan. The plan should include the following: •define critical recovery times; •identify key staff responsible for directing the recovery process, performing the recovery process, and testing recovery results; •document critical equipment needed in the recovery process and where the equipment can be obtained; •document the recovery process; •identify key reports needed to validate the success of the recovery process; and •document the process for testing the success of the recovery process. Once a full recovery plan is developed, a copy should be moved to a secure offsite location that is owned or leased by the University along with the | | |
<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></td>
<td></td>
<td></td>
<td>necessary backup files. The recovery plan should be tested, and procedures established to ensure the plan is kept up-to-date. Backup files should also be moved to an off-site location.</td>
<td></td>
</tr>
</tbody>
</table>

# of Items 2

**Total:** 10
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 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

Department of Mechanical Engineering (September 2008)

Previous Quarter Evaluation

Current Quarter Evaluation

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

Previous Quarter Evaluation

Current Quarter Evaluation

PCI Compliance (December 2009)

AudienceView Assessment
Lessons Learned
PCIDSS Monitoring
Risk Assessment
Information & Communication Monitoring
Control Environment

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

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

Control Environment
Monitoring
Information & Communication
Risk Assessment
Admin/Financial Review
Sponsored Projects
Purchasing & Disbursements
Gift Expenditures
Payroll/Personnel
Controlled Substances

Potential
Over-Control
Desirable
Control Level
Adequate Control
Significant Control Level
Critical Control Level
Google Apps for UMN (January 2010)

Office of Student Finance (January 2010)
Units with Charts that Fully Implemented their "Essential" Recommendations During the Past Quarter

Original Report Evaluation

Previous Quarter Evaluation

Current Quarter Evaluation

College of Biological Sciences (February 2008)

College of Food, Agricultural, and Natural Resource Sciences (July 2008)

[Adequate Control] [Significant Control Level] [Critical Control Level] [Potential Over-Control]
A Review of Capital and HEAPR Projects Funded by 2006 State General Obligation Bond Debt (September 2008)

- Control Environment
- Monitoring
- Information & Communication
- Risk Assessment
- Expense Allowability
- Statutory Compliance
- Cost Transfers
- Cash Draws

OIT Security & Assurance (February 2009)

- Control Environment
- Monitoring
- Information & Communication
- Risk Assessment
- Security Policy
- Security Education
- Security Operations

Legend:
- Adequate Control
- Significant Control Level
- Critical Control Level
- Potential Over-Control
UMD Labovitz School of Business & Economics (March 2010)

Original Report Evaluation

Previous Quarter Evaluation

Current Quarter Evaluation

Control Environment
Monitoring
Information & Communication
Risk Assessment
Cash Receipts & Receivables
Disbursements
Payroll
Information Systems
Sponsored Projects

Desirable
Control Level
Potential
Over-Control

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

NO PREVIOUS CONTROL EVALUATION CHART
Audit Activity Report

Scheduled Audits

- Completed audits of: University Services IT, a review of fringe benefit cost components, OIT Change Control, OIT Administration, UMD Facilities Management, the CFANS Research and Outreach Centers, and a University-wide review of employee performance evaluation processes. Details are shown on the following charts.

- Began/continued audits of: Sponsored Financial Reporting, the University’s Procurement Card Program, Veterinary Diagnostic Labs, Boynton Health Service, UMD University Relations, the Office of Real Estate Management, CLA IT management, OIT Data Network, an Executive Officer expense review, and a review of small dollar vendor payment transactions.

Investigations

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

- Issued a report on a review of the Upward Bound Program in the College of Education and Human Development. Details are shown on the following chart.

Special Projects

- Provided consulting services related to: data security, Google HIPAA compliance, data center management and consolidation efforts, Audience View cut over to a hosted solution, software as service standard, institution continuity planning, the In Common Silver federation project, identity management tool RFI project, BioSafety Level 3 lab security, 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
  - Research Compliance Committee
  - Executive Compliance Oversight Committee
  - Institutional Conflict of Interest Committee
  - Information Technology Collegiate Leaders Audit Finding Taskforces
  - Collegiate IT Directors Committee
  - 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
Audit Reports Issued Since June 2010

University Services IT

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Desirable Control Level</td>
<td>Critical Control Level</td>
<td>Potential Over-Control</td>
<td>Adequate Control</td>
<td>Significant Control Level</td>
<td>Good</td>
<td>Adequacy of MAP</td>
<td>Satisfactory</td>
<td></td>
</tr>
</tbody>
</table>

University Services Information Technology (USIT) is well managed. Leaders have sound strategies and strive to adhere to University policies. USIT has demonstrated a commitment to providing enterprise class service and support. This commitment is shown by aligning with University goals in a measured and deliberate manner. University Services’ servers and workstations are reasonably secure, but require specific controls for the management of privileged users. USIT has a good code change management process, but lacks a process to ensure that only authorized and tested changes are moved into production. Greater control is required over 3rd party services. Disaster recovery planning and testing are not complete, but a project is underway to help ensure that this will be done by November 2010.

Fringe Benefit Cost Review

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Monitoring</th>
<th>Information &amp; Communication</th>
<th>Risk Assessment</th>
<th>Cost Components</th>
<th>Internal Admin Costs</th>
<th>Rate Development</th>
<th>Fringe Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desirable Control Level</td>
<td>Critical Control Level</td>
<td>Potential Over-Control</td>
<td>Adequate Control</td>
<td>Significant Control Level</td>
<td>Good</td>
<td>Adequacy of MAP</td>
<td>Satisfactory</td>
</tr>
</tbody>
</table>

Report # 1017  Issue Date Jun-10
# of Essential Recs. 2  Total # of Recs. 7
Overall Assessment Good Adequacy of MAP Satisfactory

From the results of the audit work performed on fringe benefit costs and rate development, we believe central units including Office of Human Resources (Employee Benefits), Controller’s Office (Accounting Services) and the Budget Office have developed a control environment and a system of internal control that addresses most major business and compliance risks. Additional monitoring is obtained through the use of third party auditors and external consultants.
This review was initiated at the request of the College of Education and Human Development because of concerns regarding the operations of the program. TRIO Upward Bound is a college preparatory program for low-income and educationally disadvantaged high school students. Key elements of effective internal control were found to be deficient. Interviews conducted suggest a dysfunctional control environment with significant trust and communication concerns creating an environment not conducive to compliance. The seriousness and volume of concerns identified also reflect an overall lack of oversight and understanding of policies and programmatic responsibilities on the part of program management. The continuing or recurring nature of some of the reported issues also suggests the need for more vigilant oversight and sustainable controls to ensure future compliance.

Implementation of the Integrated Change Control process has fundamentally changed how system changes are made in OIT. There has been significant improvements in the control environment, and risks associated with system changes have already been substantially reduced. Work still remains to meet OIT’s stated goals of alignment, transparency, and effective communication with stakeholders. While some tools are in place to prevent or detect unauthorized or untested changes from being moved into production, the tools and processes vary by type of system change and in some cases by the system/application. The process for managing and controlling emergency changes has not been fully defined. Business process owners are not always involved or directly represented in the change management process.

- **Upward Bound**
  - **Report #**: 1102
  - **Issue Date**: Sep-10
  - **# of Essential Recs.**: 16
  - **Total # of Recs.**: 26
  - **Overall Assessment**: Needs Improvement
  - **Adequacy of MAP**: Satisfactory

  The control environment was found to be deficient during interviews, with concerns regarding the operations of the program. Key elements of effective internal control were found to be deficient. Interviews conducted suggest a dysfunctional control environment with significant trust and communication concerns creating an environment not conducive to compliance. The seriousness and volume of concerns identified also reflect an overall lack of oversight and understanding of policies and programmatic responsibilities on the part of program management. The continuing or recurring nature of some of the reported issues also suggests the need for more vigilant oversight and sustainable controls to ensure future compliance.

- **OIT Change Control**
  - **Report #**: 1103
  - **Issue Date**: Sep-10
  - **# of Essential Recs.**: 2
  - **Total # of Recs.**: 5
  - **Overall Assessment**: Good
  - **Adequacy of MAP**: Satisfactory

  Implementation of the Integrated Change Control process has fundamentally changed how system changes are made in OIT. There has been significant improvements in the control environment, and risks associated with system changes have already been substantially reduced. Work still remains to meet OIT’s stated goals of alignment, transparency, and effective communication with stakeholders. While some tools are in place to prevent or detect unauthorized or untested changes from being moved into production, the tools and processes vary by type of system change and in some cases by the system/application. The process for managing and controlling emergency changes has not been fully defined. Business process owners are not always involved or directly represented in the change management process.
OIT's $70 million annual expenditures account for approximately 30% of all technology expenditures. Central University allocations account for 60% of OIT's financial resources. OIT complies with all reporting requirements established by University Budget and Finance. OIT seeks to be transparent in several ways, including: posting service statements and regularly meeting with key University clients. However, OIT should seek to further improve transparency through capturing and reporting more detailed financial information on costs related to services, enterprise applications and inter-institutional arrangements. OIT should also seek to be more transparent with how sources of technology revenue, including end of year carryforward balances, are being generated and used.

UMD FM administration has displayed a commitment to strong internal controls. The operational and financial controls within Facilities Management are generally effective. Considering the length of time since the last audit of FM, we feel the issues in this report are not indicative of serious deficiencies in the control environment. The only essential recommendation addresses the need for proper separation of accounts receivable duties.
CFANS Research and Outreach Centers and the Cloquet Forestry Center

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Monitoring</th>
<th>Information &amp; Communication</th>
<th>Risk Assessment</th>
<th>Cash Receipts, AR, ISOs</th>
<th>Disbursements &amp; Purchasing</th>
<th>Payroll and Personnel</th>
<th>Sponsored Projects</th>
<th>Inventories</th>
<th>Information Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Report # | 1106 | Issue Date | Sep-10 | # of Essential Recs. | 8 | Total # of Recs. | 21 | Overall Assessment | Good | Adequacy of MAP | Satisfactory |

The mission of the ROCs is to optimize the unique resources of strategically placed living laboratories to conduct basic and applied research, outreach, and engagement. Improvement is needed over the controls and processes in several areas, most notably in payroll since salaries account for a large portion of expenses at each of the locations. We also identified the need for improved controls related to internal and external sales. In addition, improvements in controls are needed for the contingent fund checking accounts used at each location.

Performance Evaluation Review

Due to the scope of this audit we did not develop a control evaluation chart.

Report # | 1107 | Issue Date | Sep-10 | # of Essential Recs. | 0 | Total # of Recs. | 3 | Overall Assessment | Good | Adequacy of MAP | Satisfactory |

Board of Regents policies state that, “the University is committed to assessing and supporting the development of the behavioral and functional competence of its employees, consistent with expressed academic and administrative needs, the role of the employee, and performance expectations”. In our opinion, performance evaluations are adequately conducted and monitored consistent with Office of Human Resources expectations through a combined effort by academic administrators and HR directors at the unit/college/department levels and by the Office of Human Resources.
Audit Committee

October 7, 2010

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:

Baker Tilly Virchow Krause, LLP was engaged by the College of Continuing Education to conduct an audit of the financial statements of University radio station KUOM 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 $9,900 plus out of pocket expenses. This engagement does not impair the independence of Baker Tilly Virchow Krause, LLP as related to their ability to perform external audits of the University. The engagement was reviewed and approved by the Controller's Office in conformance with Board of Regents policy.

Deloitte & Touche LLP was engaged by the University to conduct a close-out audit of a sponsored project awarded to the School of Journalism and Mass Communications in the College of Liberal Arts. This audit is required by the sponsor, the Minnesota Department of Employment and Economic Development. The fees for this engagement are not to exceed $8,000. This engagement does not impair the independence of Deloitte and Touche LLP as related to their serving as independent external auditor for the University of Minnesota. The engagement was reviewed and approved by the Controller's Office in conformance with Board of Regents policy.
Background Information:

Engagements with external auditors that do not require prior approval by the Board of Regents are reported after the fact to the Audit Committee as information items, in conformance with Board of Regents policy, *Audit Committee Charter*. 