November 26, 2018

TO: The Board of Trustees of the University of Oregon

FR: Angela Wilhelms, Secretary

RE: Notice of Executive and Audit Committee Meeting

The Executive and Audit Committee of the Board of Trustees of the University of Oregon will hold a public meeting on the date and at the location set forth below. Subjects of the meeting will include: the quarterly audit report and recommended changes to the internal audit charter; the semi-annual enterprise risk management report, and an update on Transform IT and Information Systems’ security efforts.

The meeting will occur as follows:

**Monday, December 3, 2018 at 2:00 p.m.**
Ford Alumni Center, Giustina Ballroom

The meeting will be webcast, with a link available at [www.trustees.uoregon.edu/meetings](http://www.trustees.uoregon.edu/meetings).

The Ford Alumni Center is located at 1720 East 13th Avenue, Eugene, Oregon. If special accommodations are required, please contact Jennifer LaBelle at (541) 346-3166 at least 72 hours in advance.
Convene
- Call to order, roll call
- Approval of September 2018 EAC minutes (Action)


2. Transform IT Update: Jessie Minton, Vice Provost and Chief Information Officer

3. Quarterly Audit Report and Suggested Amendment to Audit Charter (Action): Trisha Burnett, Chief Auditor

Meeting Adjourns
Agenda Item #1

Enterprise Risk Management
Strategic Enterprise Risk Management and Compliance Committee Report

University of Oregon Board of Trustees

December 2018
Overview

The Strategic Enterprise Risk Management and Compliance (SERMC) committee is charged by the President of the University. The committee charge is to:

1. Develop tools and processes to actively identify, evaluate, and manage university risks
2. Ensure that systems and processes are in place to provide accountability for compliance with the University’s legal and policy obligations
3. Encourage communications, problem-solving, and collaboration across divisions, units, and departments

The committee is chaired by:
- Chief Resilience Officer and Associate Vice President for Safety and Risk Services

Committee membership includes:
- Vice President for Finance and Administration and Chief Financial Officer
- Vice President for Research and Innovation
- Vice President and General Counsel to the University
- Vice President for Equity and Inclusion
- Vice President for Student Life
- Vice President for Student Services and Enrollment Management
- Vice President for University Communications
- Vice President for University Advancement
- Executive Vice Provost for Operations
- Vice Provost for Information Services and Chief Information Officer
- Chief Resilience Officer and Associate Vice President for Safety and Risk Services
- Chief Human Resources Officer and Associate Vice President for Human Resources
- Chief Auditor
- Associate Vice President for Business Affairs and University Controller
- Senior Associate Vice President for Research and Innovation
- Director of Intercollegiate Athletics

Committee members serve as risk area leads or “risk owners” over the potential risk exposure areas, conditions or events that exist in their portfolios.

In 2017-2018 the committee asked risk owners and subject matter experts within their portfolios to review and provide feedback on their risk exposure areas and to identify existing controls and mitigation strategies.

In order to increase situational awareness among leadership and management, risk owners also gave presentations on their risk areas at one of the monthly SERMC meetings. The committee also established a work group structure to address emerging risks.
2018 University Institutional Risk Profile

Continuous Review
Risks that have the potential for a HIGH or VERY HIGH impact and have a HIGH or VERY HIGH likelihood of occurring

Continuous Monitoring
Risks that have the potential for a LOW or MODERATE impact and a HIGH or VERY HIGH likelihood of occurring

Periodic Review
Risks that have the potential for a HIGH or VERY HIGH impact and a LOW or MODERATE likelihood of occurring

Periodic Monitoring
Risks that have the potential for a LOW or MODERATE impact and a LOW or MODERATE likelihood of occurring
SERMC Work Groups
When SERMC identifies potential gaps or risk exposures that do not have a risk owner or that require additional in-depth analysis the committee establishes inter-departmental and cross-disciplinary work groups to explore the concern. The groups focus primarily on topics that require special attention for purposes of compliance, planning response, or risk management. SERMC provides the work group with a clearly defined charge, a set of expected outcomes, and a timeline for the work group to return to the committee with recommendations.

Work Group Process: from risk identification to action

The work group approach allows SERMC to bring campus partners to the table to better understand specific risk exposures, and to develop actionable recommendations to mitigate those risks. The work group structure also encourages information sharing, problem-solving, and collaboration across divisions, units and departments.
Information Communications Technology Accessibility Work Group

SERMC charged this work group to:

- Bring together stakeholders to develop strategies for removing barriers and improving accessibility of information and communication technologies (ICT) across campus (including UO websites, web pages, and web applications among others).
- Identify and review current policies/procedures/practices regarding accessible technologies at UO.
- Finalize an ICT Accessibility Policy and Procedures (including implementation guidelines) for submission to the Policy Advisory Council.
- Research methods to ensure information provided by or gathered from third-party vendors is accessible, including standards and language related to ICT procurement.

Membership:

- Human Resources
- General Counsel
- Information Services
- Student Services and Enrollment Management
- University Communications
- Accessible Education Center
- Purchasing and Contracting Services
- UO Libraries
- Office of the Registrar
- Athletics
- Student Life
- Business Affairs

Findings:

- The work group recommended that the University dedicate more resources to ensure that all UO web pages and other active ICT be made accessible to the widest range of users, including those with disabilities.

Actions:

- The work group created an accessibility link on the uoregon.edu home pages that directs individuals to a website where inquiries, requests, and complaints can be submitted. The website is https://www.uoregon.edu/accessibility.
- The work group drafted a policy and procedures to address ICT compliance at the University. There is one provision in the procedures that speaks to a proposed implementation schedule that is contingent on an external audit of all outward facing University websites. The Office of Internal Audit is currently exploring potential external auditors for this purpose. The group anticipates another recommendation to SERMC to approve the phases and costs of an audit.
- The work group recommended development of a proposal for the Budget Advisory Group to fund a new position (ICT Accessibility Program Manager) who would specialize in ICT compliance. SERMC agreed to the proposal. The work group is developing a budget proposal for FY20.
Special Events on Campus Work Group

SERMC charged a Special Events on Campus work group to research and recommend institutional policies and procedures for safeguarding special events hosted on campus by the university and/or unaffiliated groups.

**Membership:**
- Safety and Risk Services
- Risk Management
- Emergency Management
- Athletics
- UO Scheduling and Event Services
- UO Fire Marshal’s Office
- UO Police Department
- University Communications
- Student Life
- Campus Planning and Facilities Management
- Business Affairs
- Purchasing and Contracting

**Findings:**
- Events that are scheduled through UO Scheduling are well monitored and vetted.
- Event booking procedures managed by UO Scheduling are not formalized.
- Many groups independently oversee their own buildings. The decentralized nature of how space is managed increases the likelihood that an event will not be vetted, associated risks will not be mitigated, and that the campus will not receive campus-wide communications about the event.
- The university does not use a centralized scheduling software to manage space reservations across campus. A request for proposals (RFP) for software packages is needed.
- Resources for planning events live in a number of locations depending on the types of event needs (e.g., space reservations, alcohol permits, fire safety, security, etc.)
- Fees for third party space rentals are not assessed consistently.
- Certain very large scale events require the coordination of many departments across campus and are a drain on resources.

**Actions**
- UO Scheduling worked with General Counsel to improve and finalize event scheduling procedures.
- The university acquired centralized scheduling software that will allow for enterprise wide visibility into all events on campus.
- General Counsel developed event procedure templates and shared them with Schools and Colleges who manage their own spaces.
- Student Life is beginning to develop a one-stop website that will contain all of the information needed for developing, scheduling, and hosting special events.
Nighttime Safety Training, Outreach and Engagement Work Group

SERMC charged this work group to:
1. Catalog existing personal safety and assault prevention awareness and training resources provided by campus partners.
2. Explore ways to link, align and leverage modes of outreach, engagement, and trainings related to nighttime safety and violence prevention. Develop a short-term action plan to enhance safety messaging and trainings for fall of 2018 in order to reach a broader audience using multiple tools.

Membership:
- Safety and Risk Services
- Student Life
- Student Services and Enrollment Management
- UO Police Department
- Human Resources
- University Communications
- Dean of Students

Findings:
- Current personal safety and assault prevention awareness resources are dated.
- There is no centralized location for the various resources (websites, videos, etc.).
- Outreach and training efforts around safety and violence prevention awareness on campus are decentralized by department.

Actions:
- The work group recommended that new safety and violence prevention awareness training videos need to be launched. Safety and Risk Services oversaw the launch of a safety campaign about the UO app and University Communications produced safety and violence prevention awareness training videos.
- The work group recommended that the UO mobile app should be used to aggregate the various safety and violence prevention awareness trainings websites already in place. The group also created a new button on the UO mobile app for emergency contacts.
- The work group recommended, and SERMC agreed, that the Chief Resilience Officer should be the steward of the safety portion of the UO mobile app.
Nighttime Safety Transportation Program Work Group

SERMC charged this work group to:
1. Catalog existing nighttime campus transportation programs and near campus transportation (e.g., Lane Transportation District, etc.).
2. Explore opportunities to improve services and/or develop new or alternative ways to address campus nighttime transportation needs.

Membership:
- Office of the Vice President for Finance and Administration
- Safety and Risk Services
- Parking and Transportation
- UO Police Department
- Student Life
- Community Relations
- Campus GIS and Mapping

Findings:
- There are numerous nighttime transportation options currently available including Designated Driver Shuttle, Saferide, Bike Share, Spring Break airport pickup, UOPD escort, LTD, and taxis.
- The fixed route shuttle does not have long term funding. The service was discontinued at the end of spring term 2018.
- Ride share options such as Uber and Lyft are coming to Eugene soon. It is unclear what impact this will have on nighttime transportation options.
- LTD does not have capacity to take on a fixed route shuttle system similar to the system that was put in place following the string of robberies in spring 2018.
- LTD may further reduce services used by the campus community.
- The Campus Transportation Plan is more than 30 years old and does not address the issue of nighttime transportation.

Actions:
- SERMC was presented with different options and recommended that a temporary shuttle service will run in the 2018-2019 academic year. The president provided one-time funds for the temporary shuttle service.
- The work group recommended that a timeline and strategy be developed to identify current transportation needs and that the Campus Transportation Plan be updated accordingly.
- In September 2018, the UO Department of Parking and Transportation began working on a Strategic Plan to mature and improve programs and customer service. Parking and Transportation will soon begin work on a long-range campus master plan that will assess infrastructure needs, operations, capital projects, and funding options.
- Safety and Risk Services and Campus GIS Mapping created an app on the UO mobile app called “UO Rides” that allows users to view maps and see on and off campus transportation options.
In Progress and Upcoming SERMC Work Groups

Nighttime Safety Campus and Near Campus Lighting Work Group: This work group builds on the annual campus safety walk and explores opportunities to expand the current campus safety route map to include near off-campus buildings, Greek Life housing, near campus housing, etc. This group is also working with the City of Eugene, near campus neighborhood associations, and businesses to explore collaborative efforts/projects to increase the amount of nighttime lighting. Recommendations and a short-term action plan should be complete in December of 2018.

Enterprise Training Coordination and Systems Work Group: This work group will help SERMC better understand the breadth of current training tools at UO and on which platforms the tools are maintained. The work group will look at streamlining how trainings are offered, managed, and tracked. The work group will also explore strategic operational and direct cost saving strategies.

University Reporting Channels: The University has multiple channels for reporting concerns (e.g., fraud, safety concerns, persons in imminent risk of suicide, technology accessibility, academic misconduct, etc.). This work group will identify the reporting channels currently in place and explore options for centralizing enterprise-wide reporting channels. In addition, the group will catalog potential high-risk activities in which physical contact is within the scope of professional duties. The group will assess the required certifications for performing high risk activities of this type.
Agenda Item #2

Transform IT and Information Services Update
Information Technology Update

Date: December 3, 2018

Board of Trustees of the University of Oregon

Presented by:

Jessie Minton, Vice Provost for Information Services and Chief Information Officer
Information Technology Priorities – AY 2018-2019 and Beyond

**Foundational IT Maturity**
- Transform IT
  - IT Strategic Plan “Excellence through Technology”
  - Cybersecurity Strategic Plan “SecureU”
  - Network redesign
  - Project management maturity

- Online/hybrid education environment
- Emphasize student success in technology choices
- Use tech to meet students where they are

- High speed research connectivity
- Oregon Fiber Partnership – regional high speed connectivity
- Research services
  - Scalable and secure cloud services
  - On-premise services

**Enabling Education & Student Success**

- Project management maturity

**Enabling Research**

2019  2020  2021  2022
Agenda

• Transform IT
• SecureU
Transform IT: program that will rationalize the use of information technology resources on campus to better support the University of Oregon’s strategic academic and research missions.

**Summer 2017:**
- Determined and defined service based approach for program
- Defined project management methodology and governance

**Fall/Winter 2017:**
- Created documentation, reports by unit of previous IT consulting engagements
- Hired project management and business analysis staff

**Spring/Summer 2018:**
- Launched campus engagement phase
  - Service inventory, cost, staffing, gap analysis

**Fall/Winter 2018 - 2020:**
- Service migrations based upon IT charter and advancement of UO mission
52 unique IT units were identified

**Academic and Administrative:**
28 academic and administrative IT units identified and asked to provide estimates of their annual IT budgets which included:

- Staff (+ OPE) Budget
- Student Employee Budget
- Operational Budget (Hardware and Software)

**Research:**
24 research IT units identified and asked to share how they received IT services and the greatest areas of need for their work
$14m of current general fund budget resides centrally in Information Services, roughly 29%
The greatest area of desired interest for the research community:

*Programmatic support or consultation*

The next most needed services were:
- Data backup
- Storage solutions
- Website development
- Application development
- Desktop support
NEXT STEPS
<table>
<thead>
<tr>
<th><strong>Service List</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Applications</strong></td>
</tr>
<tr>
<td><strong>Server/System Administration</strong></td>
</tr>
<tr>
<td><strong>Computer Lab Management</strong></td>
</tr>
<tr>
<td><strong>Equipment Checkout</strong></td>
</tr>
<tr>
<td><strong>Training</strong></td>
</tr>
<tr>
<td><strong>Consult/Project Admin</strong></td>
</tr>
</tbody>
</table>
## Services recommended out of scope

<table>
<thead>
<tr>
<th>Business Applications</th>
<th>Help Desk</th>
<th>Desktop Support</th>
<th>Network Management</th>
<th>Classroom &amp; AV Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>Software &amp; Applications</td>
<td>Websites</td>
<td>Accounts &amp; Access</td>
<td>Information Security</td>
</tr>
<tr>
<td>Computer Lab Management</td>
<td>Telephone</td>
<td>Email &amp; Calendaring</td>
<td>Printing</td>
<td>Purchasing</td>
</tr>
<tr>
<td>Equipment Checkout</td>
<td>Teaching &amp; Learning</td>
<td>Ed Tech Consulting</td>
<td>Data Center/Server Closet</td>
<td>File Sharing</td>
</tr>
<tr>
<td>Training</td>
<td>Storage</td>
<td>Video Conferencing</td>
<td>Knowledge Management</td>
<td>Data Backup</td>
</tr>
<tr>
<td>Consult/Project Admin</td>
<td>Instant Messaging</td>
<td>Digital Signage</td>
<td>IT Strategic Planning</td>
<td></td>
</tr>
</tbody>
</table>

**Rationalization not recommended** | **In scope for related project**
Phase 1 recommendation – in scope

<table>
<thead>
<tr>
<th>Business Applications</th>
<th>Help Desk</th>
<th>Desktop Support</th>
<th>Network Management</th>
<th>Classroom &amp; AV Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/System Administration</td>
<td>Software &amp; Applications</td>
<td>Websites</td>
<td>Accounts &amp; Access</td>
<td>Information Security</td>
</tr>
<tr>
<td>Computer Lab Management</td>
<td>Telephone</td>
<td>Email &amp; Calendaring</td>
<td>Printing</td>
<td>Purchasing</td>
</tr>
<tr>
<td>Equipment Checkout</td>
<td>Teaching &amp; Learning</td>
<td>Ed Tech Consulting</td>
<td>Data Center/Server Closet</td>
<td>File Sharing</td>
</tr>
<tr>
<td>Training</td>
<td>Storage</td>
<td>Video Conferencing</td>
<td>Knowledge Management</td>
<td>Data Backup</td>
</tr>
<tr>
<td>Consult/Project Admin</td>
<td>Instant Messaging</td>
<td>Digital Signage</td>
<td>IT Strategic Planning</td>
<td></td>
</tr>
</tbody>
</table>
Phase 1 recommendation – in scope

Consolidate disparate services to create new offering:
User Support Services
Phase 1 recommendation – in scope

Rationalize related services as one effort

Storage

Video Conferencing

Knowledge Management

Data Backup

Consult/Project Admin

Instant Messaging

Digital Signage

IT Strategic Planning

Equipment Checkout

Training

Consult/Project Admin

Instant Messaging

Digital Signage

IT Strategic Planning
Each business application will require individual assessment.
### Timing for Phase 1

<table>
<thead>
<tr>
<th>Date Range</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 2018</td>
<td>Steering committee support ITSC Support</td>
</tr>
<tr>
<td>Dec 2018</td>
<td>Planning Stakeholder engagement</td>
</tr>
<tr>
<td>Jan-April 2019</td>
<td>User support services (USS) project kickoff Business process documentation</td>
</tr>
<tr>
<td></td>
<td>Storage and backup planning/kickoff</td>
</tr>
<tr>
<td>April 2019</td>
<td>Present new USS service delivery model Begin USS implementation Business applications kickoff</td>
</tr>
<tr>
<td>2019 – early 2020</td>
<td>USS Implementation Establish new org structures Subsequent services kickoff</td>
</tr>
</tbody>
</table>
Vision

A knowledgeable and capable UO community working together to safeguard our digital assets and capabilities to empower excellence in research and instruction in a resilient cyber environment.

Mission

To empower the UO community to leverage digital assets and capabilities, and defend our cyber environment through proactive measures.
### Current Risks

<table>
<thead>
<tr>
<th>UO Impact</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Probably</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R1</td>
</tr>
<tr>
<td>Large</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R2</td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R3</td>
</tr>
<tr>
<td>Small</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insignificant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Sample attacks against UO:

- **2018:** 15,000+ students, faculty, staff passwords potentially stolen (653 confirmed); **Tracking Cost (1,300 Hours, $80K); sensitive data came within grasp** of attacker(s)

- **2016-2017:** Theft of 60+ faculty DuckIDs/Passwords
High-Risk Weaknesses

Access Control
- DuckID / Password is inadequate
- 95 / PAC is woefully inadequate

Awareness
- 15,000+ phished users (Aug ‘18)
- 60+ phished faculty (Oct ‘16)

Data Security Compliance
- Unmanaged system security vulnerabilities
- High-Risk Data proliferation
- Insufficient guidance
Solution to High-Risk Weaknesses

Access Control
2-Factor Authentication:
Student Health, Student Conduct, DuckWeb, Banner, Privileged Access, ...

Awareness Training
Email Security
- Online Training for All
- Self-Phish for faculty/staff
- In-person Training

Data Protection Security Framework
- Vulnerability Scanning & remediation
- Data Loss Prevention
- Data Security Framework
# Round 1 – Minimum Investment to Reduce High-Risk Weaknesses

<table>
<thead>
<tr>
<th>Function</th>
<th>Benefit</th>
<th>Description</th>
<th>Investments</th>
</tr>
</thead>
</table>
| **2-Factor Authentication (P1)** | • 98% end-user breach reduction  
• Reduce impact of incidents | **19,000 users** (non-student affiliations)  
• Hardware Tokens (non-cell phone users)  
• Telephony Credits  
• IT Support (1 FTE)  
• IT Service Management (1 FTE)  
• Professional service  
• Project Mgmt. & Business Analyst FTE | $16K  
$34K  
$32K  
$95K  
$127K  
$34K  
$32K |
| **Awareness Training (P2)** | • Reduce susceptibility to and impact of phishing  
• Targeted training | **Online Training Modules** (all users)  
**Self-Phishing tool** (faculty and staff) | $55K  
$14K |
| **Vulnerability Scanning (P3)** | • Find vulnerabilities before the adversary | **Vulnerability Scanning Tool**  
**Cybersecurity Analysts** (1 FTE)  
**Professional Services**  
**Project Mgmt. & Business Analyst FTE** | $6K  
$75K  
$8K  
$152K |
| **Data Loss Protection (P4)** | • Curtail insecure data storage  
• Increase guidance via Data Security Framework | **Data Loss Prevention Tool** (DLP)  
**Cybersecurity Analysts** (0.5 FTE)  
**Professional Services**  
**Project Mgmt. & Business Analyst FTE** | ---  
---  
$16K  
$23K |
| **Incident Monitoring & Response (P5)** | • Increase incident visibility & response | **Cybersecurity Operating Center** (CSOC) Equipment (student-run) | $25K |
| **Total Investment** | | | **$140K**  
**$718K** |
## Round 2 – Minimum Investment to Reduce Compliance Risks

<table>
<thead>
<tr>
<th>Function</th>
<th>Benefit</th>
<th>Description</th>
<th>Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Protection (P1)</strong></td>
<td>• Reduce breach/disruption like ransomware</td>
<td>• Software</td>
<td>$139K</td>
</tr>
<tr>
<td></td>
<td>• Protect data and increase compliance</td>
<td>• IT Support (1 FTE)</td>
<td>$117K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Professional Services</td>
<td>$20K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Project Mgmt. &amp; Business Analyst FTE</td>
<td>$32K</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk &amp; Compliance Management (P2)</strong></td>
<td>• Increase proactivity and compliance with HIPAA, GLBA, GDPR, FERPA, NIST 800-171, ...</td>
<td>• Cybersecurity Analysts (1 FTE)</td>
<td>$150K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cybersecurity Interns &amp; GE’s (3)</td>
<td>$59K</td>
</tr>
<tr>
<td><strong>Training - Security, IT (P3)</strong></td>
<td>• Increase defense capability of cybersecurity staff</td>
<td>• Ongoing training for cybersecurity staff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support guided DIY cybersecurity to broaden scope and capability university-wide</td>
<td>• Ongoing cybersecurity training for IT staff and Cybersecurity Liaisons</td>
<td>$35K</td>
</tr>
<tr>
<td><strong>Miscellaneous Analysis Tools (P4)</strong></td>
<td>• Reduce impact of malware</td>
<td>• Malware analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enhance email security</td>
<td>• Email security addition</td>
<td>$5K</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Investment</strong></td>
<td></td>
<td></td>
<td>$57K</td>
</tr>
</tbody>
</table>

**Recurring Investment**

- $503K
## Round 3 – Investment to Increase Compliance & Address Growth

<table>
<thead>
<tr>
<th>Function</th>
<th>Benefit</th>
<th>Description</th>
<th>Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GDPR Compliance Management (P1)</strong></td>
<td>- Streamline responses to GDPR rights requests; reduce risk of hefty fines</td>
<td>- Coordinate GDPR compliance activities</td>
<td>$12K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project Mgmt. &amp; Business Analyst FTE</td>
<td>$14K</td>
</tr>
<tr>
<td><strong>Risk &amp; Compliance Management (P2)</strong></td>
<td>- Increase proactivity and compliance with HIPAA, GLBA, GDPR, FERPA, NIST 800-171, ...</td>
<td>- Cybersecurity Analyst (0.5 FTE)</td>
<td>$75K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cybersecurity Interns &amp; GE’s (2)</td>
<td>$40K</td>
</tr>
<tr>
<td><strong>Data Loss Prevention Expansion</strong></td>
<td>- Curtail insecure data storage</td>
<td>- Data Loss Prevention Tool Expansion</td>
<td>$58K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project Mgmt. &amp; Business Analyst FTE</td>
<td>$23K</td>
</tr>
<tr>
<td><strong>SIEM Expansion (P3)</strong></td>
<td>- Augment staffing levels by leveraging big data analytics; increased incident detection and response</td>
<td>- Expand to address increased campus coverage and growth of network traffic</td>
<td>$25K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Professional Services</td>
<td>$16K</td>
</tr>
<tr>
<td><strong>NetFlow Analysis Expansion (P4)</strong></td>
<td>- Quick detection and response to incidents</td>
<td>- Network analysis to detect and map paths of incidents; expansion to address traffic growth</td>
<td>$15K</td>
</tr>
<tr>
<td><strong>Computer Forensics Tool (P5)</strong></td>
<td>- Limit reporting/notification by uncovering actual incident impact</td>
<td>- Forensically-sound investigations to support UOPD, VPRI, Audit, OGC, plus security incidents</td>
<td>$2K</td>
</tr>
<tr>
<td><strong>Total Investment</strong></td>
<td></td>
<td></td>
<td>$68K $227K</td>
</tr>
</tbody>
</table>
SecureU Next Steps

November 2018
- IT Steering Committee
- Strategic Risk Management Committee

Gain endorsement

Dec 2018/Jan 2019
- Strategic Budget Allocation Process

Request Funding

Jan/Feb 2019
- Two-factor Authentication
- Awareness Training

Begin Implementation

**Requested Funding**

<table>
<thead>
<tr>
<th>Year</th>
<th>One-Time</th>
<th>Recurring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>$140K</td>
<td>$718K</td>
</tr>
<tr>
<td>Year 2</td>
<td>$57K</td>
<td>$503K</td>
</tr>
<tr>
<td>Year 3</td>
<td>$68K</td>
<td>$227K</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>$265K</strong></td>
<td><strong>$1,448K</strong></td>
</tr>
</tbody>
</table>
Questions?
Agenda Item #3

Quarterly Audit Report
&
Proposed Changes to the Internal Audit Charter

The quarterly audit report will be provided as a supplemental document as soon as it is finalized.
The Board of Trustees is asked to consider changes to the charter of the Office of Internal Audit (OIA).

In order to comply with the Quality Assurance and Improvement Program (QAIP) requirements, OIA conducted a review of the standing internal audit charter, last amended by the Board in June 2017. The existing charter was compared to the latest Quality Assessment Manual, which provides industry standards and best practices. After that review, OIA suggests certain changes to ensure required components are included and greater clarity around language.

Pursuant to the policy on board committees, the Executive and Audit Committee can act on this resolution on behalf of the full board; a seconded motion is not required.
Resolution: Amendments to the Internal Audit Charter

Whereas, the University of Oregon is governed by and the business and affairs of the University are ultimately managed by the Board of Trustees;

Whereas, the University of Oregon takes seriously the responsibility to manage, invest and spend resources and has an Office of Internal Audit (Internal Audit) to provide independent, objective evaluations and advisory services that add to the accountability of the University;

Whereas, Internal Audit has a departmental charter to articulate the purpose, authority, and responsibility of the office;

Whereas, Internal Audit proposes an update to the charter, attached hereto as Exhibit A, to (i) better align the document with current Quality Assurance Review requirements and (ii) ensure consistency with best practices in higher education audit environments; and,

Whereas, the Board’s Policy on Committees authorizes the Executive and Audit Committee to act on behalf of the Board when appropriate;

NOW, THEREFORE, the Executive and Audit Committee of the Board of Trustees of the University of Oregon hereby adopts the updated Internal Audit Department Charter attached as Exhibit A.

Moved: ___________  Seconded: _________

<table>
<thead>
<tr>
<th>Trustee</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bragdon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ford</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kari</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lillis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ralph</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wilcox</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Dated: ___________  Recorded: _________
EXHIBIT A: REDLINE VERSION OF PROPOSED CHANGES

Office of Internal Audit

Department Charter

This charter defines the purpose, authority, and responsibility of the Office of Internal Audit at the University of Oregon

June 2017 - December 2018

Approved by the University of Oregon Board of Trustees Executive and Audit Committee

June 1, 2017 - December 3, 2018
**Purpose**

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve university operations. It helps the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The Office of Internal Audit enhances and protects the University’s value by providing risk-based and objective assurance, advice, and insight.

**Mission Statement:**

Driven by the highest professional and ethical standards, the Office of Internal Audit helps the University accomplish its objectives by evaluating and identifying opportunities to improve the effectiveness of governance processes, risk management, and internal controls.

**Professional Standards:**

The responsibility of the Office of Internal Audit operates within the context of its service to the University in a manner that is consistent with the standards established by the internal audit community. At a minimum, it shall comply with the Institute of Internal Audit’s (IIA’s) Auditors’ (“IIA”) mandatory guidance including the **Definition of Internal Auditing**, the **Code of Ethics** and the **International Standards for the Professional Practices Framework** (Practice of Internal Auditing (“IPPF”) and the Office of Internal Audit’s procedure manual. Audits will be conducted with integrity, objectivity, confidentiality, and competency as defined by the IIA’s Code of Ethics.”).

Additionally, the Office of Internal Audit references other appropriate audit frameworks, such as the Generally Accepted Government Auditing Standards.

The Office of Internal Audit will undergo external peer reviews pursuant to the IPPF. The Executive and Audit Committee shall have input into peer reviews and results of peer reviews will be available to the Committee upon completion.

**Authority**

To ensure the independence of the Office of Internal Audit, the Chief Auditor reports administratively to the Office of the President and functionally to the Executive and Audit Committee of the University of Oregon’s Board of Trustees. **The Chief Auditor will provide quarterly progress reports to the Executive and Audit Committee at each regular meeting, summarizing the results of engagement activities and reports. In addition, the Chief Auditor will keep the President, campus leadership, and the Executive and Audit Committee apprised of high-risk engagement issues.**

The Office of Internal Audit is granted full and unrestricted access to all functions, records, systems, property, and personnel. Any documents or information obtained by the Office of Internal Audit through the course of work will be handled with the confidentiality defined by the IIA’s Code of Ethics. The Office of Internal Audit has authority to audit any function, program, account or system deemed necessary and appropriate in the judgment of the Chief Auditor, notwithstanding a flexible pre-approved audit plan.

University management is responsible for risk management, control, and governance of the areas audited. The Office of Internal Audit has no direct responsibility or authority over any of the areas audited. Staff shall not perform any operational duties for the University, initiate or approve accounting transactions of areas under review, or direct the activities of any University employee, except to the extent such employees have been appropriately assigned to an audit team or to otherwise assist the auditors.

All university employees are expected to comply fully and timely with requests made by the Office of Internal...
Audit. This includes, but is not limited to, timely provision of information, access to information, or responses to draft reports. Recommendations made by the Office of Internal Audit shall be taken seriously and steps shall be taken to assess and determine a course of action in response to the recommendations. The Chief Auditor may report any non-compliance on the part of university programs or employees to the President and the Executive and Audit Committee.

**Responsibility**

The Office of Internal Audit is responsible for developing and implementing a flexible annual audit plan using an appropriate risk-based methodology. The annual audit plan should include consideration of any risks or control concerns identified by management, and should be reviewed and approved by the President and Executive and Audit Committee.

The Office of Internal Audit shall perform engagements in the following areas:

- **Assurance services:** These services are independent and objective evaluations designed to provide reasonable assurance regarding the achievement of objectives over the effectiveness and efficiency of operations, reliability of financial reporting, or compliance with applicable laws and regulations.

- **Consulting services:** These services may be requested by managers and other department and unit leaders to help identify a variety of areas for improvement. The scope and objectives are agreed upon by the Office of Internal Audit and management of the area.

- **Investigative services:** These services evaluate allegations of fraud, waste, abuse or unethical business practices. The Fraud and Ethics Hotline is free, confidential, and available to employees, students, and the community to report unlawful or unethical concerns. Operated by Ethics Point, reports are managed by the Office of Internal Audit. Reports can also be made directly to the Office of Internal Audit.

- **Other services:** These services include coordination and oversight for external auditing agencies, and follow-up work. External auditing agencies include agencies such as the Secretary of State and the NCAA. Follow-up work is performed within the context of the IPPF to ensure plans and actions are taken to correct report conditions. Additionally, the Office of Internal Audit provides awareness training covering topics such as fraud, risks, and internal controls.
Office of Internal Audit
Quarterly Report

December 2018

Report to the Board of Trustees of the University of Oregon
Executive and Audit Committee
TABLE OF CONTENTS

Summary ............................................................................................................................................ 2
Completed Projects ............................................................................................................................. 3
Projects in Progress............................................................................................................................ 3
Ongoing Projects ............................................................................................................................... 4
Upcoming Projects .............................................................................................................................. 4
Follow-Up Projects ............................................................................................................................ 4
Hotline Summary ............................................................................................................................... 5
Administrative..................................................................................................................................... 6

SUMMARY

The Office of Internal Audit ("Internal Audit") provides a quarterly report to assist the President and the Executive and Audit Committee with their oversight responsibilities for Internal Audit.

Internal Audit works to complete projects from the approved audit plan while meeting administrative goals for the year. The office currently has one vacant auditor position and is in the process of starting a search. Due to the turnover, some projects that were in process during the prior quarter are still in process. Consulting projects are also accepted by management request in an effort to proactively address risks and increase efficiencies across campus.

During the previous quarter, Internal Audit presented to an audience of peers at both regional and national conferences. This not only aligned with Internal Audit’s strategic plan, but also offered the unique opportunity to discuss audit strategies, specific to the University, with a large group of peers. Internal Audit also presented about internal controls and fraud at the University’s Financial Stewardship Institute.

Finally, after a successful partnership with student members of Beta Alpha Psi during the previous Spring term, a new group of students has been selected for the coming Winter and Spring terms. Internal Audit has also hired a student intern.

If there are any questions regarding the content of this report, I am available for discussion. Thank you for your work and your continued support of Internal Audit.
COMPLETED PROJECTS

ASSURANCE
Athletics IT Assessment
Internal Audit, in collaboration with Baker Tilly, began this project in February 2018. This project was identified on the approved FY18 audit plan. The objective was to conduct an IT assessment for the Athletics department covering key people, processes, and technology used. Opportunities to strengthen information technology general controls within Athletics were identified.

CONSULTING
There were no consulting projects finalized during the quarter.

PROJECTS IN PROGRESS

ASSURANCE
Non-retaliation Policies
Internal Audit began this project in August 2017. This project was identified on the approved FY18 audit plan. The objective is to evaluate the compliance and effectiveness of current University policies governing retaliatory behavior. This project has been reassigned to the Chief Auditor for completion due to turnover. One challenge affecting completion has been the need to identify all reporting channels on campus. As of August 2018, a management workgroup has been established for this purpose. This project is currently in the reporting phase. Estimated completion: December 2018

Cash Handling
Internal Audit began this project in September 2017. This project was rolled over from the fiscal year 2017 approved audit plan to the approved FY18 audit plan. The objective is to evaluate the internal control structure of the processes governing cash handling across campus, as established by the Business Affairs Office ("BAO"). The project is in the reporting phase, pending an exit conference with management for final report issuance. Estimated completion: December 2018

I-9 Compliance
Internal Audit, in collaboration with students from Beta Alpha Psi, began this project in April 2018. This project was identified on the approved FY18 audit plan. The objective is to evaluate the University's compliance with I-9 requirements during the hiring process. The project is in the reporting phase, pending an exit conference with management for final report issuance. Estimated completion: December 2018

Human Resources (HR) Practices and Controls
Internal Audit, in collaboration with Baker Tilly, began this project in May 2018. This project was identified on the approved FY18 audit plan. The objective is to evaluate the effectiveness of processes within the central function. This project is currently in the fieldwork phase. Estimated completion: February 2019

Firearms Inventory
Internal Audit began this project in September 2018. This project was identified on the approved FY19 audit plan. The objective is to verify that all firearms purchased by the University of Oregon Police Department are tracked, accounted for, and properly registered as required. This project is currently in the final planning phase. Estimated completion: March 2019

University Health Center IT Assessment
Internal Audit, in collaboration with Baker Tilly, began this project in October 2018. This project was identified on the approved FY19 audit plan. The objective is to conduct an IT assessment for the University Health Center covering key people, processes, and technology used. This project is currently in the final planning phase. Estimated completion: March 2019
**Payment Card Industry (PCI) Program Assessment**
Internal Audit, in collaboration with Baker Tilly, began this project in October 2018. This project was identified on the approved FY19 audit plan. The objective is to review and assess the University’s program for complying with PCI Data Security Standards (DSS) requirements. This project is currently in the planning phase. *Estimated completion: March 2019*

**Inventory of Critical Business Functions**
Internal Audit began this project in September 2018. This project was identified on the approved FY19 audit plan. The objective is to perform an assessment of where and how decentralized critical business processes occur at the University. This project is currently in the planning phase. *Estimated completion: June 2019*

**CONSULTING**
Internal Audit is currently working on three consulting projects for different units on campus that are at various stages of completion. While these projects take time away from planned assurance projects, they serve three very important purposes, 1) to improve efficiencies and effectiveness in a proactive manner, 2) to reinforce Internal Audit’s purpose to be a valuable partner, and 3) to provide Internal Audit with more insight regarding campus risks. Areas addressed in the current year include internal controls, process improvement, and identification of efficiencies. Once finalized, reports are issued summarizing any recommendations.

**ONGOING PROJECTS**

*Consulting:* As mentioned previously, consulting projects are performed at management’s request. The FY19 audit plan includes time for these activities. This is an area that Internal Audit has emphasized and pursued heavily. As opportunities arise, Internal Audit offers this service and it has been well received by the University community. Internal Audit continues to offer training on internal controls, risk, and fraud awareness and presents at the annual Financial Stewardship Institute. Additionally, Internal Audit has developed a training series on the COSO Internal Control Framework to be offered through the Professional Development initiatives in Human Resources. Internal Audit offers facilitated internal control self-assessments as a service for the campus, as well as continues campus outreach and presentations to reach new audiences and introduce new concepts.

*External Audit Coordination:* Internal Audit is charged with coordinating and providing oversight for other control and monitoring functions, including external audit. Moss Adams, LLP is the external firm responsible for the university’s financial statement audit, single audit, and NCAA agreed upon procedures. During the past quarter, Internal Audit met with Moss Adams to continue collaboration and information sharing. Internal Audit also assisted Sponsored Project Services with the R&D Single Audit conducted by Moss Adams.

**UPCOMING PROJECTS**

**ASSURANCE**

*Vendor Reviews*
Internal Audit, in collaboration with students from Beta Alpha Psi, is scheduled to begin this project in December 2018. This project was identified on the approved FY19 audit plan. The objective is to verify appropriate contracts are in place, as required. *Estimated completion: April 2019*

*NCAA Compliance*
Internal Audit is scheduled to begin this project in December 2018. This project was identified on the approved FY19 audit plan. The objective is to evaluate the effectiveness of the program using a compliance framework. *Estimated completion: April 2019*

**NCAA Ticket Count**  
Internal Audit is scheduled to begin this project in December 2018. This project is a routine audit identified on the approved FY19 audit plan. The objective is to verify average minimum attendance per the NCAA Division I requirements. *Estimated completion: February 2019*

**CONSULTING**  
Three consulting project requests have been received and are set to begin next quarter.

**FOLLOW-UP PROJECTS**

To comply with internal auditing standards that require monitoring of audit recommendations communicated to management, Internal Audit performs follow-up projects. The objective is to ensure corrective actions on the audit recommendations, including those that may have been considered non-reportable, have been effectively implemented by management, or that management has accepted the risk of not taking action.

**COMPLETED**  
**Follow Up of Lab Safety Practices**  
Internal Audit followed up on eight observations and 26 management corrective actions. Of the corrective actions, 24 have been completed, while the remaining two are in progress. The final report was issued the first week of September. Internal Audit will follow up on the two remaining corrective actions during the first quarter of FY20.

**Follow Up of Printing and Mailing Services**  
Internal Audit followed up on 20 observations and 20 management corrective actions. Of the corrective actions, 13 have been completed, three are in process, three have not been started, and one has been accepted. The final report was issued the last week of November. Internal Audit will follow up on the two remaining corrective actions during the first quarter of FY20.

**Consulting Follow Ups**  
Internal Audit conducts follow-ups for consulting projects to determine whether corrective actions on recommendations have been effectively implemented by management and whether Internal Audit can provide additional assistance. Internal Audit is currently working on three consulting projects follow-ups.

**UPCOMING**  
There are two audit follow-up projects scheduled for the upcoming quarter.

**HOTLINE SUMMARY**

Internal Audit has received the following requests for investigative services during the current fiscal year. Of these, three are in progress, and four has been referred to other units. Note that those referred to other units are followed up on by Internal Audit to ensure appropriate disposition.

<table>
<thead>
<tr>
<th>Reporting Sources for FY19 Investigative Services</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus Direct to Internal Audit</td>
<td>2</td>
</tr>
<tr>
<td>3rd Party Hotline</td>
<td>5</td>
</tr>
<tr>
<td>Grand Total</td>
<td>7</td>
</tr>
</tbody>
</table>

It is common for a university our size to have an active hotline. Peer institution benchmarking indicates the activity is low for our institution, but has improved from the prior fiscal year. Internal Audit is working with leadership on additional ways to market this tool. In addition, Internal Audit is working to inventory other reporting mechanisms that may exist on campus.

**ADMINISTRATIVE**

Internal Audit continues to work on the Strategic Plan implementation schedule. Outreach on campus and involvement in national organizations were conducted during the prior quarter. Implementation of internal control, risk, compliance and fraud trainings and resource templates for units are in progress.