UNIVERSITY OF
OREGON

December 2, 2019

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 set forth below. The subjects of the meeting will be: internal audit quarterly report and charter amendments, and board officers.

The meeting will occur as follows:

Monday, December 9, 2019 at 3:00 p.m.
Ford Alumni Center | Giustina Ballroom

The meeting will be webcast, with a link available at https://trustees.uoregon.edu/meetings.

The Ford Alumni Center is located at 1720 East 13th Avenue, Eugene, Oregon. Sign language for the deaf or hard of hearing should be requested at least 48 hours in advance of the posted meeting time by contacting Jennifer LaBelle at (541) 346-3166 or emailing trustees@uoregon.edu. Please specify the sign language preference.

UNIVERSITY OF OREGON

Board of Trustees | Executive and Audit Committee
Public Meeting | December 9, 2019 | 3:00 p.m.
Ford Alumni Center | Giustina Ballroom

Convene

- Call to order, roll call
- Approval of June and September 2019 EAC minutes (Action)

1. **Internal Audit – Quarterly Audit Report, IT Risk Assessment Refresh, and Proposed Amendments to the Audit Charter (Action):** Amy Smith, Interim Chief Auditor

2. **Board Officer Nominations (Action):** Peter Bragdon, Trustee

Meeting Adjourns

UNIVERSITY OF OREGON

Agenda Item #1

Internal Audit Quarterly Report & Audit Charter Amendments

INTERNAL AUDIT CHARTER: PROPOSED AMENDMENTS

Summary of Proposed Action

The Office of Internal Audit (OIA) proposes minor adjustments to the Internal Audit Charter. OIA routinely reviews the charter for alignment with industry best practices. Most recently, the charter was reviewed as part of the OIA's required Quality Assurance and Improvement Program (QAIP). The charter was reviewed against the industry's Quality Assessment Manual. The proposed edits ensure required components from the QAM are included and provide some clarification to existing language. The amendments appear in Exhibit A to the resolution, which is at the end of this section of the packet. The Executive and Audit Committee may take action on this matter on behalf of the full Board.

In this packet, preceding the resolution and associated redline, you will find the quarterly audit report and the IT Risk Assessment "refresh" report from Baker Tilly.

UNIVERSITY OF OREGON

Office of Internal Audit
Quarterly Report

December 2019

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

TABLE OF CONTENTS

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. Consulting projects are also proposed by campus units, and are prioritized based on audit staff capacity in an effort to proactively address risks and increase efficiencies across campus.

During the previous quarter, Internal Audit finalized two assurance projects. In addition, there are five assurance projects and three consulting projects in progress at various stages of completion. Follow up projects are also performed to ensure previous audit recommendations have been followed, and risks have been appropriately addressed; two follow up projects are in progress now.

If there are any questions regarding the content of this report, the interim Chief Auditor is available for discussion. Thank you for your work and your continued support of Internal Audit.

COMPLETED PROJECTS

ASSURANCE

Payment Card Industry (PCI) Program Assessment

Internal Audit, in collaboration with Baker Tilly, performed this project. This project was identified on the approved FY19 audit plan. The objective was to review and assess the University's program for complying with PCI Data Security Standards (DSS) requirements. Internal Audit concluded that the PCI program is well coordinated and focused on meeting the compliance requirements. Three recommendations were made for further improvement of the PCI program. The final report was issued in September 2019.

IT Risk Assessment Refresh

Internal Audit, in collaboration with Baker Tilly, performed this project. This project was identified on the approved FY20 audit plan. The objective was to refresh the enterprise-wide IT risk assessment that was completed in FY16 in order to identify and prioritize University IT risks. Internal Audit validated and agreed with the majority of identified University IT risk exposures currently documented and tracked by the Strategic Enterprise Risk Management and Compliance ("SERMC") committee. Additionally, the investments made by the University in IT over the past two and half years have reduced specific IT risk areas. Two recommendations were made for improving the University's IT risk assessment and exposure. The final report was issued in November 2019.

CONSULTING

There were no consulting project finalized during this quarter.

FOLLOW-UPS

There were no follow-up projects finalized during this quarter.

PROJECTS IN PROGRESS

ASSURANCE

Critical Business Functions

Internal Audit began this project in September 2018. This project was identified on the approved FY19 audit plan as a result of systemic risks identified by Internal Audit. These risks were communicated to senior leadership and the Board of Trustees. The objective is to perform an assessment of where and how decentralized critical business operational processes occur at the University. This project is currently in the reporting phase. *Estimated completion: December 2019*

Ticket and Parking Sales Processes

Internal Audit began this project in April 2019. This project was identified on the approved FY19 audit plan. The objective is to evaluate the adequacy of controls over reporting and accountability for ticket and parking sales. This project is currently in the reporting phase. *Estimated completion: December 2019*

Physical to Cyber

Internal Audit, in collaboration with Baker Tilly, began this project in March 2019. This project was added to the FY19 audit plan. The objective is to evaluate the security practices of high risk physical-to-cyber systems and validate adherence to UO's policies and procedures and industry leading security practices. This project is currently in the fieldwork phase. *Estimated completion: January 2019*

Data Governance

Internal Audit, in collaboration with Baker Tilly, began this project in October 2019. This project was identified on the approved FY20 audit plan. The objective is to assess the data governance practices at the University based on leading higher education practices for data governance. This project is currently in the planning phase. *Estimated completion: February 2020*

Vendor Reviews

Internal Audit, in collaboration with a student employee and students from Beta Alpha Psi, began this project in December 2018. This project was identified as a Tier II project on the approved FY19 audit plan. The objective is to assess whether contracts were authorized, appropriate, and in accordance with University policies and procedures. This project is currently in the reporting phase. *Estimated completion: Project placed on hold due to staff turnover.*

CONSULTING

Internal Audit is currently working on three consulting projects for different units on campus that are at various stages of completion. The most notable current consulting project is a process review in SPS to ensure controls are in place for compliance with grant requirements. 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.

FOLLOW-UPS

To comply with internal auditing standards that require monitoring of audit recommendations communicated to management, Internal Audit performs follow-up projects. The objective of follow up projects is to monitor the disposition of observations from prior projects. Internal Audit ensures corrective actions on the project 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.

Follow Up of Purchasing Practices

Internal Audit is following up on six observations that included 13 corrective action items from Purchasing and Contracting Services (PCS) included the original report. This follow-up is being conducted in conjunction with the Vendor Contract Review audit. *Estimated completion: Project placed on hold due to staff turnover.*

Follow Up of Lab Safety Practices

Internal Audit conducted an initial follow-up in September 2018 of 26 corrective actions. Twenty-four corrective actions were completed and two remained in progress. Internal Audit is currently following up on the two remaining corrective actions. *Estimated completion: January 2020*

UPCOMING PROJECTS

ASSURANCE

NCAA Ticket Count

Internal Audit is scheduled begin this project in December 2019. This project is a routine audit identified on the approved FY20 audit plan. The objective is to verify average minimum attendance per the NCAA Division I requirements. *Estimated completion: February 2019*

Admissions

Internal Audit plans to begin this project once FY19 audit projects are complete. The audit focus is to evaluate the processes used to admit students, including consistency of decision making and classifications.

CONSULTING

There are three consulting projects that have been requested, however due to staff turnover and lack of available resources, these consulting projects have been placed on hold.

FOLLOW UP

Printing and Mailing Efficiencies

Internal Audit conducted an initial follow-up in November 2018 of 20 corrective actions. Fourteen corrective actions were completed, three remained in progress, and three had not been started. Internal Audit will be following up on the six remaining corrective actions.

Grant Management Processes

Internal Audit plans to begin this assurance follow up once FY19 audit projects are complete. This project is a follow up of an audit performed in FY15.

HOTLINE SUMMARY

Internal Audit has received the following reports for investigative services during FY20. Of these, 12 are open.

Reporting Sources for FY20 Investigative Services	
Campus Direct to Internal Audit	1
3rd Party Hotline	13
Grand Total	**14**

For FY19, the following requests for investigative services were received. Of these, 11 are closed, and 11 are open.

Reporting Sources for FY19 Investigative Services	
Campus Direct to Internal Audit	9
3rd Party Hotline	13
Grand Total	**22**

Note that some of these reports have been referred to other units for review and potential investigation. Reports referred to other units are followed up on by Internal Audit to ensure appropriate disposition.

It is common for a university our size to have an active hotline. We have seen an increase the past quarter from prior fiscal years. A SERMC workgroup, in which Internal Audit is a member, has been working to inventory and streamline reporting channels that may exist on campus.

ONGOING PROJECTS

Consulting: In addition to the previously mentioned consulting projects, Internal Audit provides the following advisory services to campus:

- Advice and trainings on internal controls, risk and fraud awareness. A training was presented on Internal Controls and Fraud at the annual Financial Stewardship Institute.
- Facilitation of internal control self-assessments for units
- Serves on various University committees and workgroups. Examples include, SERMC, DSIRT, ISPGC, etc.

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 coordinated with Moss Adams, Business Affairs and Research on the financial statement audit and research & development (R&D) single audit.

ADMINISTRATIVE

Internal Audit is undergoing personnel changes due to turnover in the Chief Auditor role. As of August 15, 2019, the Senior Auditor was appointed as the Interim Chief Auditor and is serving in that capacity while a national search is conducted.

University of Oregon

FY 2020 Information Technology ("IT") Risk Assessment

November 2019

bakertilly

Report delivered to:

- Patrick Phillips, Provost and Senior Vice President
- Michael Schill, President, University of Oregon
- Angela Wilhelms, Secretary of the University, Board of Trustees
- Kevin Reed, Vice President/General Counsel
- Jamie Moffitt, Vice President for Finance and Administration/Chief Financial Officer
- Jessie Minton, Vice Provost for Information Services and Chief Information Officer
- Leo Howell, Chief Information Security Officer

Baker Tilly Virchow Krause, LLP trading as Baker Tilly is an independent member of Baker Tilly International. Baker Tilly International Limited is an English company. Baker Tilly International provides no professional services to clients. Each member firm is a separate and independent legal entity, and each describes itself as such. Baker Tilly Virchow Krause, LLP is not Baker Tilly International's agent and does not have the authority to bind Baker Tilly International or act on Baker Tilly International's behalf. None of Baker Tilly International, Baker Tilly Virchow Krause, LLP nor any of the other member firms of Baker Tilly International has any liability for each other's acts or omissions. The name Baker Tilly and its associated logo is used under license from Baker Tilly International Limited.

Executive Summary

Background

Driven by the highest professional and ethical standards, the Office of Internal Audit ("Internal Audit") helps the University of Oregon (the "University" or "UO") accomplish its objectives by evaluating and identifying opportunities to improve the effectiveness of governance processes, risk management, and internal controls. Baker Tilly, an accounting and advisory firm, works with Internal Audit to provide co-sourced IT internal audit services.

During fiscal year ("FY") 2016, Baker Tilly conducted an IT risk assessment that involved identifying IT risks for the University. The constantly changing IT landscape is a dynamic threat requiring constant attention. To mitigate risks, protect data, and facilitate compliance, the University must be able to manage known risks and identify new ones. As such, the University's IT risk assessment must be occasionally updated to reflect the changes in the IT environment.

Objective and Scope

Baker Tilly refreshed the results of the FY16 IT risk assessment and created a list of potential future IT audit projects. The scope of the assessment encompassed, at a high level, all IT risks to University systems and data, as well as the supporting people, processes, and technology.

Results

Based on our analysis of information gathered, stakeholder responses, and higher education industry specific information, we validated and agreed with the majority of the identified University IT risk exposures currently documented and tracked by the Strategic Enterprise Risk Management and Compliance ("SERMC") committee. Baker Tilly did identify two recommendations for improving the IT risk exposures, related to decentralized IT and data management (See the Recommendations section for details).

Additionally, the investments made by the University in IT over the past two and a half years have reduced specific IT risk areas (See University IT Changes section for details). The changes in risk are noted on the IT risk map later in the report.

Approach

To conduct the assessment, Baker Tilly used a three step approach. This approach was centered on the University's IT risks and was supported by ongoing collaboration and project management between Baker Tilly and the University. Specifically, Baker Tilly conducted the following:

I. Planning
   a. Developed a high-level project plan and timeline
   b. Confirmed with Internal Audit the stakeholders to interview

II. Fieldwork
   a. Conducted interviews with stakeholders to review existing IT risks and determine new risks that have emerged since the prior IT risk assessment was conducted
   b. Requested and reviewed documentation, as appropriate
   c. Analyzed information gathered, stakeholder responses, and higher education industry specific information and updated IT risks, as needed

III. Reporting
   a. Developed a draft written report updating the IT risk assessment results
   b. Obtained feedback on draft IT risk assessment report from stakeholders and UO senior leadership
   c. Finalized report and presented results to senior leadership and the Executive and Audit Committee of the Board of Trustees

University IT Changes

In the years since the prior formal IT risk assessment was conducted by Baker Tilly in 2015, the University has made several improvements that have translated into strategic and technical strengths for the University's IT environment. The following significant changes, all of which have been accomplished in the previous two and a half years, are programs, initiatives, and improvements that have led to positive change and help to reduce the potential impact and likelihood of certain IT risk exposures. For each of these changes, we have noted the associated IT risk areas that have been impacted, thus reducing IT risk exposure to the University.

Governance

The University has established an IT governance structure that is three-tiered. At the top level of the governance structure is the IT Steering Committee, which advises the Provost on matters related to IT policies, priorities, and performance. The committee is supported by a set of subcommittees and advisory boards, which advise on specific areas such as academic, research, and administrative technologies. The governance structure has enabled the alignment of IT decisions with the University's mission, improved communication among the IT community, provided assurance to stakeholders, and better integrated risk management into IT decision making. ***IT risk area(s) impacted: IT Governance***

Strategic Hires

The University has made many significant strategic IT hires since 2017. Specifically, Jessie Minton was hired as the Chief Information Officer ("CIO"), Leo Howell was hired as the Chief Information Security Officer ("CISO"), and Matt Riley was hired as the Chief Technology Officer ("CTO"). The leadership of these individuals has improved IT operations and strengthened Information Services' ("IS") position in the University as a strategic partner to help achieve the University's mission. ***IT risk area(s) impacted: Information Security and Privacy, IT Governance, Infrastructure – Network***

Cybersecurity

Since coming to the University in 2017, Leo Howell, CISO, has developed a cybersecurity strategic plan. In May 2019, the University's Budget Advisory Group approved a financial investment that will go toward improvements in campus-wide cybersecurity defense, including one-time funds for immediate cybersecurity needs and recurring funding to improve technology systems to protect the University from cyber attacks. ***IT risk area(s) impacted: Information Security and Privacy, Funding***

Transform IT Initiative

Transform IT is the University's program to rationalize the use of information technology resources on campus to better support UO's strategic academic and research missions. The University currently has many IT departments on campus, resulting in inefficient use of resources, fragmentation of work, and duplication of tools, processes, and services. Additionally, there is disparity among academic, research, and administrative units with regard to the levels of service each area receives. The Transform IT initiative has already made changes to IT service delivery (e.g., reorganization of classroom technology support). Specifically, the Center for Media and Educational Technologies ("CMET") units have moved under IS. The College of Arts and Science Information Technology ("CASIT") group has also been reorganized to fall under IS. Current Transform IT projects are designed to further the maturity of IT services while creating equity in core IT services provided. The rationalization of services should result in savings across the University that can be strategically reinvested. The program is also meant to establish effective governance and organizational structures and provide transparency for IT investments. ***IT risk area(s) impacted: People Resources, End User Support, Technology Choice, Device Management***

Academic and Administrative Technology

The University has recently enabled many software platforms for enhanced collaboration. The Campus Email Project is a multi-year effort to move all UO students, faculty, and staff to a single email service, UOmail (i.e., Microsoft Office 365). Previously, approximately 20 different email platforms were used and supported across campus. The benefits of this project include consistent collaboration tools (e.g., efficient meeting scheduling, real-time messaging, and document collaboration), as well as enhancements to resilience, reliability, and security. Additionally, multiple classroom technology platforms were previously in place across campus; a consistent platform was installed and redundant systems were eliminated to help reduce technical debt. Finally, a request for proposal is in process for a new constituent relationship management ("CRM") tool to replace the current multiple CRM systems with one comprehensive solution. ***IT risk area(s) impacted: Academic Computing, Enterprise Applications***

Network Infrastructure Investments

Significant investments have been made to improve network infrastructure since FY17. Through the strategic investment process, IS received strategic funding to replace and upgrade the aging network infrastructure with modern technology (e.g., cabling upgrades, wireless network improvement/expansion, core networking upgrades). For example, IS upgraded the network bandwidth between the University and external parties in 2018, connecting to the Internet2 national network at 100GB to enable transfers of big data off campus. These network infrastructure efforts are on-going and will continue into the next few fiscal years. Additionally, Jessie Minton, CIO, is a founding board member and the treasurer of Link Oregon, which is a non-profit consortium of the State of Oregon and the state's research institutions that "seeks to enhance research, innovation, health care, education, and public services across the state," by providing high-speed, fiber-optic broadband connectivity to the state's non-profit and public sectors. ***IT risk area(s) impacted: Infrastructure – Network, Information Security and Privacy, Funding***

Themes

During our work in FY16, we noted themes related to distribution of IT and optimization of IT resources across the University. While the University has made improvements in these two areas since FY16, these themes remain important and relevant in FY20. Additionally, we have identified a new theme in FY20 specific to organizational change management. Presented below, at a summary level, are the overarching themes that were observed during our review.

Distribution of IT

IT services are delivered to faculty, staff, students, and other University community members by various unique IT units. While not all IT units provide the same types or levels of services, many of the services are duplicated across IT units (e.g., end user support, application development). In addition to the distribution of IT services across the IT units at UO, there are numerous instances of IT units collaborating to provide services to other functional areas of the University, some of which have a dedicated IT unit and others that do not. As such, IT risks and challenges in one IT unit can affect many of the other IT units due to the level and complexity of the collaboration between IT units.

Optimization of IT Resources

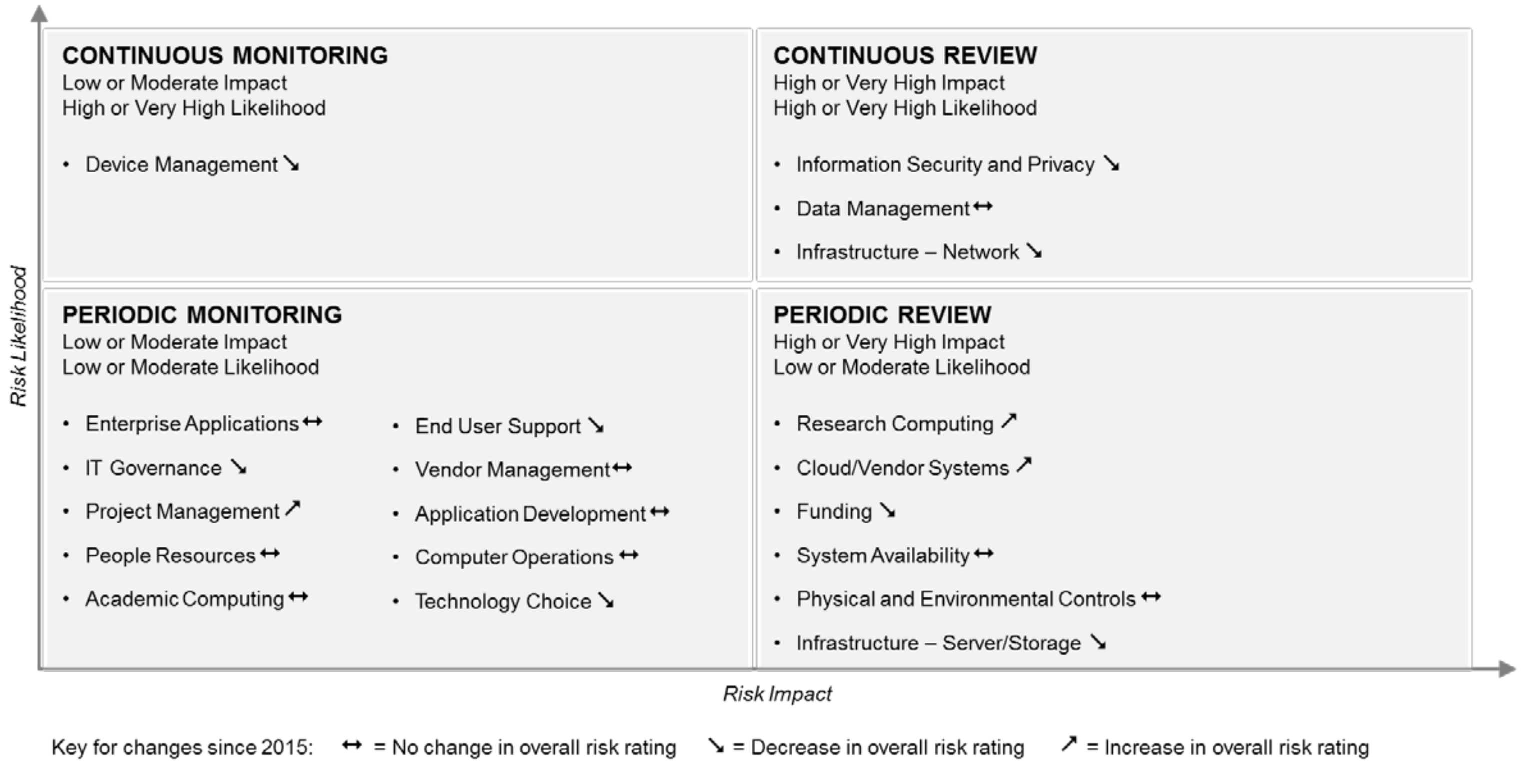
As a result of the decentralized model of IT services, which has grown organically over time, both personnel and budget dollars are dispersed across campus in the various IT units and are likely not optimized in terms of efficient use of resources. As such, this current structure could make it difficult to optimize people and budget resources across the University in order to address risks and support strategic initiatives.

Organizational Change Management

Historically, organizational change management activities, including processes to plan, implement, and accept new initiatives, have not been formally structured or implemented adequately. Instead, individuals have been relied upon to address change management on a project by project basis. Now, multiple major University-wide projects are underway (e.g., Transform IT, Unified Communications program), requiring the support and acceptance of various constituents (e.g., functional business areas, technologists, consultants, vendors). As such, most of the University's IT risks are impacted by organizational change management, and IT risk management activities should include components of effective organizational change management.

IT Risk Map

The University faces many IT threats as a higher education institution managing multiple networks and systems, and providing IT services to thousands of faculty, staff, students, and other constituents. The risk map below depicts the specific risk areas for UO prioritized by the potential impact and likelihood. The overall rating of risks was based on judgment, with the impact based on reputational, financial, operational, and compliance factors (see **Appendix C**), and likelihood based on potential timing of occurrence in the short, medium, or long timeframe. The placement of the risks on the risk map was based on impact and likelihood criteria used by SERMC. Refer to **Appendix A** for the criteria used for prioritizing the risk areas. The risk area descriptions can be found in **Appendix B**. ***It is important to note that these IT risk areas do not necessarily represent problems, but are risks inherent to the University's operations and the environment in which it operates.***



CONTINUOUS MONITORING
Low or Moderate Impact
High or Very High Likelihood

- Device Management ↘

CONTINUOUS REVIEW
High or Very High Impact
High or Very High Likelihood

- Information Security and Privacy ↘
- Data Management ↔
- Infrastructure – Network ↘

PERIODIC MONITORING
Low or Moderate Impact
Low or Moderate Likelihood

- Enterprise Applications ↔
- IT Governance ↘
- Project Management ↗
- People Resources ↔
- Academic Computing ↔
- End User Support ↘
- Vendor Management ↔
- Application Development ↔
- Computer Operations ↔
- Technology Choice ↘

PERIODIC REVIEW
High or Very High Impact
Low or Moderate Likelihood

- Research Computing ↗
- Cloud/Vendor Systems ↗
- Funding ↘
- System Availability ↔
- Physical and Environmental Controls ↔
- Infrastructure – Server/Storage ↘

Key for changes since 2015: ↔ = No change in overall risk rating ↘ = Decrease in overall risk rating ↗ = Increase in overall risk rating

Recommendations

Baker Tilly identified the following opportunities for improvement related to certain University IT risk exposures.

Adjusting Risk Impact

For the SERMC risk exposure “Operational Ineffectiveness – Decentralized and Uncoordinated Information Technology Environment,” Baker Tilly recommends reassessing the current noted risk impact of “High” once many of the in-process initiatives (e.g., Transform IT) are implemented in 2020.

Adding Data Management Risks

Baker Tilly recommends adding two IT risks of significance to the University’s SERMC risk exposure list. Both risks (noted below) relate to data management. Note: Data includes all forms of electronic information used for pedagogy, research, and administration at the University.

- Data policies, procedures, and standards for managing the confidentiality, integrity, and availability of institutional data are in the early stages of development and have not been fully implemented, potentially resulting in inefficient and ineffective use of data.
- Institutional data are not consistently complete, accurate, and valid during all stages of input, update, storage, and transmission, resulting in data errors that impact reporting and decision making.

Appendices

Appendix A: University of Oregon SERMC Criteria for Prioritizing Risks

Risk Impact Criteria

Scale	Definition
Very High	Core mission impaired, operationally disabling
High	Operations must shift significantly to adjust to conditions created by consequences of risk-related incident or control failure
Moderate	Operational changes are necessary to adjust to conditions created by consequences of risk-related incident or control failure
Low	Consequences of risk-related incident or control failure are tangible, but operations remain largely intact and maintain status quo

Risk Likelihood Criteria

Scale	Definition
Very High	Certain to occur
High	Almost certain to occur
Moderate	May occur within the year
Low	Not likely to occur within the year

Appendix B: IT Risk Area Descriptions

Baker Tilly identified and prioritized the following risk areas specific to the University, based on the results of our work. Each risk area is described below and listed in priority order:

- **Information Security and Privacy** – The policies, practices, and tools implemented on the University's systems and data to maintain confidentiality of information, specifically sensitive data about students, faculty, staff, donors, alumni, and research activities.
- **Data Management** – The processes and software implemented to manage, analyze, and report on data used to operate and manage the University, as well as report to external entities.
- **Infrastructure – Network** – The network hardware resources used to provide platforms for applications and databases, as well as connectivity within the University and to external resources.
- **Device Management** – The policies, practices, and tools implemented to manage, track, and secure University and personally owned laptops, desktops, phones, and tablets that collect, process, or store University data.
- **Research Computing** – The practices and tools implemented to support research computing
- **Cloud/Vendor Systems** – The process and practice of implementing new and transitioning existing IT systems and applications to the cloud or vendor managed/hosted solutions.
- **Funding** – The monetary resources allocated to acquire, maintain, and retain the people and technology resources required to operate and manage University systems.
- **System Availability** – The policies, practices, and tools implemented for maintaining the availability of systems during or after impactful events.
- **Physical and Environmental Controls** – The policies, practices, and tools used to maintain the security of and environmental protections for physical spaces containing computing resources (e.g., data center facilities
- **Infrastructure – Server/Storage** – The server hardware resources used to provide platforms for applications and databases.
- **Enterprise Applications** – The process and practice of implementing new, upgrading existing, and maintaining enterprise applications
- **IT Governance** – The processes and structure for planning, implementing, communicating, and monitoring of IT strategy to meet the University's mission and goals.
- **Project Management** – The processes and tools implemented for planning, managing, and reporting on IT projects to ensure a successful outcome.
- **People Resources** – The personnel resources, both employed and contracted, that provide IT services to various constituencies within and outside of the University.
- **Academic Computing** – The practices and tools implemented to support academic computing.

- **End User Support** – The processes and tools used to provide constituents with help desk support functions and training for University systems.
- **Vendor Management** – The policies, practices, and tools implemented to identify, contract, procure, and manage third-party IT service and product vendors.
- **Application Development** – The processes and tools used to acquire, build, test, and maintain software applications.
- **Computer Operations** – The policies, practices, and tools implemented to plan, implement, operate, change, and monitor University networks and servers.
- **Technology Choice** – The ability of leaders, managers, and end users to select from a myriad of technology solutions provided by the University or third-party vendors that can meet the requirements of their constituents.

Appendix C: Risk Impact Factors

Impact Factors	
Financial	• Loss of revenue (e.g., donations lost, grants/contracts) • Cost of response and mitigation • Financial statement audit findings
Reputation	• General public • Sponsors/donors/alumni • Students, current and potential • Faculty/staff
Operational	• Duration, frequency, and timing of key system downtime • Availability of critical information and data • Customer (e.g., faculty, staff, student) impact
Compliance	• Laws • Regulations • Contracts

Appendix D: Potential IT Audit Projects

IT Risk Area(s)	Potential IT Audit Options	Assurance Project	Advisory Project
Multiple Risk Areas	Conduct annual IT audits for departments or units that have dedicated IT personnel, focused on each unit's implementation of University policies or standards related to systems and data, as well as the specific established general IT practices within each unit.	✓	
Multiple Risk Areas	Assess compliance with federal cybersecurity requirements for research data, primarily focusing on the most common type of cybersecurity requirements, National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-53 and 800-171).		✓
Information Security and Privacy	Assess the application specific security controls used to protect data housed and processed in key systems (e.g., Banner), reviewing one key system annually.	✓	
Infrastructure - Network	Assess plans to modernize the network infrastructure, focusing on providing guidance on risks and controls that should potentially be included in project plans.		✓
IT Governance and Funding	Assess progress and effectiveness of the IT mission and goals (i.e., strategic plan), focusing on in-progress initiatives to address critical IT needs.		✓
Computer Operations	Evaluate the practices for acquiring, deploying, managing, and replacing servers, focused on key application, website, and database servers.	✓	
Device Management	Evaluate the practices for acquiring, deploying, managing, and replacing laptops, desktops, and mobile devices deployed in functional areas that handle regulated or sensitive data.		✓
Physical and Environmental Controls	Evaluate the practices for environmental protections within the physical spaces and areas housing critical IT assets (e.g., hardware, devices, data, and software) or services.	✓	

Appendix E: Contact Information

Mike Cullen, CISA, CISSP, CIPP/US
Director
(703) 923-8339
mike.cullen@bakertilly.com

Meghan Senseney
Senior Consultant
(703) 923-8469
meghan.senseney@bakertilly.com

Haley Anderson, CIA
Senior Consultant
(703) 923-8526
haley.anderson@bakertilly.com

Raina Rose Tagle, CPA, CISA, CIA
Partner
(703) 923-8251
raina.rosetagle@bakertilly.com

PAGE LEFT BLANK INTENTIONALLY

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

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 updates to the charter, attached hereto as Exhibit A, to clarify language and 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 hereto as Exhibit A.

Moved: ____________ Seconded: _________

Trustee	**Yes**	**No**
Bragdon		
Ford		
Kari		
Lillis		
Ralph		
Wilcox		

Dated: _____________ Recorded:__________

EXHIBIT A

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

December 2019

Amended and Approved by the University of Oregon
Board of Trustees Executive and Audit Committee
~~*June 1, 2017*~~
December 9, 2019

EXHIBIT A

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~~is to serve 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 written quarterly progress reports to trustees and will present at regular meetings of the Board or an appropriate committee thereof, summarizing the results of engagement activities and issued audit reports. In addition, the Chief Auditor will keep Board leadership, the President, and campus leadership, 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.

EXHIBIT A

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~~Performed within the context of the IPPF, 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~~Performed within the context of the IPPF, 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.

UNIVERSITY OF OREGON

Agenda Item #2

Board Officers

RECOMMENDATION OF BOARD CHAIR & VICE CHAIR

Summary of Requested Action

The bylaws of the University of Oregon (UO) establish officers for the Board of Trustees (Board), including a chair and vice chair. The bylaws further stipulate that terms for the chair and vice chair shall be three years (approximated based on the Board's meeting schedule). (*See* Section 5.a)

Current officers are Charles M. Lillis, chair, and Ginevra Ralph, vice chair. Both were elected to their respective positions in December 2016 with terms effective January 2017. Thus, reelection or the selection of a new chair or vice chair is timely for the December 2019 meeting.

Chair Lillis and Vice Chair Ralph expressed interest in remaining in their respective positions. No other nominations were received for either position.

The Executive and Audit Committee will discuss this matter during its meeting on December 9 and will make a formal recommendation to the full Board for consideration during the full Board meeting on December 10.

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

Resolution: Selection of Board Officers

Whereas, the bylaws of the University of Oregon (University) establish a chair and a vice chair of the board to serve as officers for the Board of Trustees (Board);

Whereas, the bylaws establish the term for board officers to be three years (or a close approximation thereof given board meeting schedules);

Whereas, the current chair, Charles M. Lillis, and vice chair, Ginevra Ralph, were elected to those positions in December 2016 with terms effective January 2017, thus rendering reappointment or the selection of new officers timely;

Whereas, Lillis and Ralph are willing to continue serving in their respective roles and trustees have expressed faith in and support for their work;

Whereas, the Executive and Audit Committee is authorized to make recommendations to the full Board of Trustees as a seconded motion.

> Now, therefore, the Executive and Audit Committee hereby recommends that the Board of Trustees of the University of Oregon reelect Charles M. Lillis as chair of the Board and Ginevra Ralph as vice chair of the Board.

Moved: ____________ Seconded: _________

Trustee	**Yes**	**No**
Bragdon		
Ford		
Kari		
Lillis	*Recused*	
Ralph	*Recused*	
Wilcox		

Dated: _____________ Recorded: _________

PAGE LEFT BLANK INTENTIONALLY