UNIVERSITY OF OREGON

Board of Trustees of the University of Oregon
Executive and Audit Committee Meeting
December 2, 2015

12:30 pm: Public Meeting, Ford Alumni Center, Room 403

Convene

- Call to order and roll call
- Approval of September 2015 EAC minutes (Action)

1. **Roles and responsibilities relating to financial integrity**, *Board Chair Chuck Lillis*

2. **Quarterly audit report**, *Interim Chief Auditor Trisha Burnett*

3. **IT risk assessment report**, *Mike Cullen, Baker Tilly LLP*

Meeting Adjourns

UNIVERSITY OF OREGON

Agenda Item #1

Roles & Responsibilities: Financial Integrity

The Administration

The university's financial health and integrity is a shared responsibility. Thousands of individuals have access to data, manage contracts, and are able to process payroll, reimbursements and other financial transactions. It is incumbent upon everyone at the institution to act responsibly and ethically.

The administration of the university bears an important and overarching duty for establishing a network of controls and a culture that allows this shared responsibility to be effective. This responsibility includes, *but is not limited to*:

- Maintaining a holistic view of the university's financial health and engaging in short- and long-term strategies to maintain the financial integrity and stability of the institution;
- Providing timely and reliable information and engaging in thoughtful, ongoing analyses of such information to identify strengths, opportunities, and potential risks;
- Establishing internal policies and procedures that ensure alignment with applicable laws, regulations and best practices for internal controls;
- Routinely evaluating policies and procedures to effectuate continuous improvement;
- Ensuring that employees undergo proper training, and have access to updated policies and procedures;
- Working collaboratively with the audit function to provide information as requested and develop – and execute – corrective actions to the extent such actions are consistent with university policy, laws and regulations, and financial feasibility;
- Communicating the importance of financial management as a shared responsibility at all levels and across all units of the institution; and,
- Continuously evaluate existing and foreseeable risks including any necessary mitigation and/or the assumption thereof.
- Holding individuals accountable for their internal control responsibilities.

Internal Audit

The internal audit function provides independent, objective assurance and advisory services that add value and accountability within the organization. The Office of Internal Audit (OIA) assists university leadership in accomplishing objectives through a systematic, disciplined approach to evaluating and recommending improvements to the effectiveness of risk management, internal controls, operations, and governance processes. OIA's work is conducted with objectivity, fairness, and in accordance with the highest professional and ethical standards.

OIA's scope of work is broad, but overall the office is focused on determining whether the university's network of governance, risk management, and control processes, as designed and represented by management, is adequate and functioning in a manner to confirm that risks are appropriately identified and managed; governance structures reflect appropriate interaction and

decision-making; information is accurate, reliable and timely; processes and employee actions are in compliance with applicable laws, regulations, and policies; resources are acquired and used economically, efficiently, and responsibly; continuous improvement is embedded in the university's operations; and significant legislative or regulatory issues are recognized and addressed. Performance of this work and the information it provides to leadership has a direct impact on the University's financial health and integrity.

External Audit

External auditors play a critical role in providing an independent validation of the university's financial information, confirming that specific laws, rules and standards governing financial reporting are followed. The external financial audit occurs annually, following each fiscal year and the completion of that year's financial statements and reports. External auditors examine controls used by the university, evidence to provide reasonable assurance that disclosures are free from material misstatement, and accounting practices and estimates to provide reasonable assurance of compliance with laws and policy.

Such external validation is required by government agencies, creditors, investors and others. Moreover, it provides the Board of Trustees and the President third-party assurance as to the control mechanisms and financial information reported.

Agenda Item #2

Quarterly Audit report

The quarterly audit report will be provided at the meeting.

Agenda Item #3

IT Risk Assessment Report

Materials will be provided at the meeting

Mike Cullen, Senior Manager

Mike Cullen is a Senior Manager with Baker Tilly, a national accounting and advisory firm. Mike leads the firm's Higher Education and Research Institution's IT risk and IT audit services team. For over 13 years, he has worked with a variety of higher education clients of various sizes, both public and private. He has led IT risk assessments and audits, developed information privacy and security programs, performed ethical hacking of IT systems, and conducted digital forensic investigations. Mike has presented to a variety of audiences, including Association of College and University Auditors (ACUA), National Council of University Research Administrators (NCURA), Society of Corporate Compliance and Ethics (SCCE), various Institute for Internal Auditors (IIA) chapters, regional, national conferences, and at multiple universities. Mike is also a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and Certified Information Privacy Professional (CIPP/US).

Raina Rose Tagle, Partner

Raina Rose Tagle leads Baker Tilly's firmwide Risk and Internal Audit Consulting Services practice, which provides industry-specialized services to the higher education, healthcare, not-for-profit, government contracting, financial services, professional services, manufacturing, government, real estate, and energy and utilities industries. Practice areas include resource optimization, financial and operational risk management, Sarbanes-Oxley compliance, fraud investigation, technology risk consulting, and organizational governance. Raina also acts as National Practice Leader - Consulting for Baker Tilly's Higher Education and Research Institutions industry practice, which provides services in financial statement audit, tax, internal audit, and strategic consulting areas such as risk management, research compliance, construction, sustainable energy, resource optimization and cost reduction, fraud prevention, talent management, and information technology. Raina serves on Baker Tilly's Growth and Retention of Women firmwide task force. Prior to joining Baker Tilly as a partner in 2006, she served as interim executive director of not-for-profit organizations and chief financial officer of a technology consulting firm; led her own consulting practice providing strategic planning facilitation, executive coaching, and organizational development; and co-founded the East Region hub of a business process outsourcing company.

Supplemental Materials

UNIVERSITY OF OREGON

Office of Internal Audit Quarterly Report

Fiscal Year 2016 – 1st Quarter

Report to the Board of Trustees of the University of Oregon
Executive and Audit Committee
December 2, 2015

TABLE OF CONTENTS

INTERNAL AUDIT ASSURANCE SERVICES

An Enterprise Risk Assessment of Information Technology (Complete)
Internal Audit outsourced audit services that require information technology expertise to Baker Tilly. The firm conducted a risk and vulnerability assessment of IT administration, operations, and security for the purpose of understanding all IT services and processes across campus, and to identify and prioritize risks associated with the University's IT environment. At this time, the risk assessment has been completed and Internal Audit is working with the firm to develop a co-sourced IT audit plan based on these results.

A Review of Purchasing Practices (In process)
Internal Audit performed a review of purchasing practices across campus to determine if procurements comply with applicable laws, and ensure fair competition. While the compliance review is still underway, opportunities to gain efficiencies and improve the effectiveness of processes were identified. Initial fieldwork was performed by the Chief Auditor before her departure. In October, this project was reassigned to the Interim Chief Auditor for completion and reporting.

A Review of Research Grant Management (In process)
Internal Audit is in the reporting phase for the review of grant management within Research and Innovation. The objective of the audit was to evaluate the grant management process within Sponsored Projects Services. Additional audit steps were conducted to assess the impact the changes to the Federal Office of Management and Budget will have on the University with respect to federal grants. Reporting is expected to be complete during the second quarter of fiscal year 2016.

Athletics Risk Assessment (In process)
Internal Audit began the initial planning phase for this project and has identified preliminary objectives. These include gaining an understanding of the athletics program in order to identify inherent risks and identifying systems and processes along with related controls that are intended to mitigate these risks. These results will be used to develop a multiple year, risk based audit plan. Due to changes in internal staffing resources, further work will be conducted once this project is reassigned.

INTERNAL AUDIT INVESTIGATIVE SERVICES

The Office of Internal Audit has conducted work on ten internal investigations based on submitted reports during the current fiscal year. Of these, five have been completed, five are in progress with two being conducted in coordination with other subject matter experts on campus.

Reporting Sources for FY16 Investigative Services	
Campus Direct to Internal Audit	6
3rd Party Hotline	4
Grand Total	**10**

INTERNAL AUDIT ADVISING SERVICES

The FY16 audit plan includes consulting activities related to awareness training, hiring practices, procurement cards, the travel process, and compliance with the Health Insurance Portability and Accountability Act. During the first quarter, Internal Audit conducted a presentation for the CAS leadership team and began developing an awareness presentation for the 2015-2016 Financial Stewardship Institute. In addition, Internal Audit consulted with the Travel Policy Advisory Group and the HIPPA compliance officer. As a result of recent turnover in the Office of Internal Audit, advising projects have been reassigned to the Interim Chief Auditor. These activities are expected to be on-going throughout the year.

EXTERNAL AUDIT COORDINATION

Moss Adams has completed their audit of the University's FY15 financial statements and will be presenting their results during the December 2015 Finance and Facilities Committee meeting. Internal Audit will continue to coordinate with Moss Adams as they finalize their work on audits related to the OMB Circular, and the NCAA Agreed-Upon Procedures.

PROFESSIONAL DEVELOPMENT ACTIVITIES

Internal Audit staff participated in the annual Pacific Northwest Higher Education Internal Audit (PNWHEIA) Conference hosted at Oregon State University in Corvallis, Oregon. The team also attended the annual Association of College and University Auditors (ACUA) Conference, during which the Chief Auditor conducted two presentations. These activities provided unique opportunities for the audit staff to obtain required CPE, enhance their knowledge, and collaborate with auditors from other higher education institutions.

STATUS OF FY16 AUDIT PLAN

The FY16 audit plan was approved by the Executive and Audit Committee in June 2015. This plan will need to be adjusted due to challenges with getting the office up-and-running, as well as staffing changes within the Office of Internal Audit that have resulted in the need to reassess the current allocation of resources. Internal Audit intends to issue a Request for Proposal for periodic internal audit support services using a co-sourced model to address these considerations.

BAKER TILLY

Candor. Insight. Results.

University of Oregon
Information Technology Risk Assessment

December 2, 2015

Table of Contents

Executive Summary

Background

After the University of Oregon (Oregon, the University, or UO) became an independent institution at the dissolution of the Oregon University System, the University hired a Chief Auditor. The Chief Auditor created the Office of Internal Audit and conducted an Enterprise Risk Assessment for the entire institution. During that risk assessment, the Chief Auditor determined the need to conduct a more detailed and focused information technology (IT) risk assessment for the entire institution due to the complex and decentralized nature of IT at Oregon.

IT risks are a natural part of any institution and may impact the ability of the University to conduct operations in support of the mission. These risks require continual assessment followed by the creation and modification of IT risk management plans. Since a formal, institution-wide IT risk assessment had not been completed in recent times, the Chief Auditor engaged accounting and advisory firm Baker Tilly, with a specialized focus in serving higher education institutions, to conduct the IT risk assessment. The assessment had three main objectives, each with a specific deliverable:

1. **Understand IT Services and Processes at Oregon**

Inventory of IT Units, Services, Key Applications, Data Types
(Provided to the Office of Internal Audit as a separate document)

2. **Identify, Prioritize, and Report on Oregon's IT Risks**

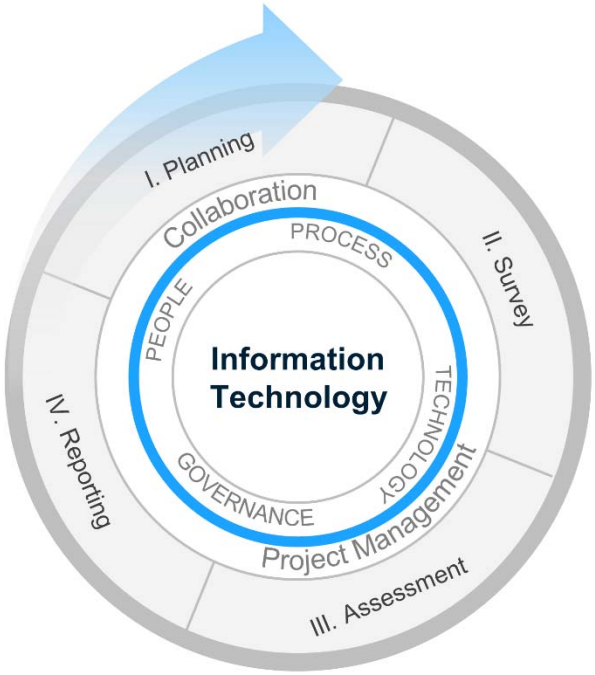
Report of Prioritized IT Risks and Summarized Observed Risks
(This document)

3. **Develop an IT Audit Plan**

Plan for IT Audits over 3-year Period
(Draft audit plan submitted to Internal Audit for continued refinement)

Approach

To conduct the assessment, Baker Tilly used a four-phased approach, represented in the graphic at right, customized to Oregon based on our initial discussions with the Chief Auditor. This approach was centered on the four aspects of IT: people, process, technology, and governance. It was also supported by ongoing collaboration and project management between Baker Tilly and the University. Specifically, Baker Tilly conducted the following:



I. Planning

- Identified initial key stakeholders (e.g., Information Services (IS), various IT directors)
- Developed a project plan for conducting the assessment
- Conducted an entrance conference with IS and initial group of IT directors
- Interviewed initially identified IT directors about their IT unit's services and processes
- Defined "IT unit" for the purpose of this assessment as: *"A function, consisting of one or more full time equivalent (FTE) positions, that provides one or more IT services (e.g., end user support, application and web development, data center management) to a distinct constituency (e.g., school, department, unit) at the University"*

II. Survey

- Conducted a data request web survey of the identified IT units to gather information about IT services, processes, and risk management strategies deployed by IT units
- Interviewed IT unit directors and certain supporting IT personnel to clarify survey responses, obtain additional information, and gather additional relevant documentation
- Reviewed documentation and artifacts from IT units
- Identified additional IT units, based on survey results and interviews, and conducted the same survey and interviews for newly identified IT units

III. Assessment

- Analyzed information and documentation gathered from IT units
- Identified and synthesized a specific set of IT risks customized to Oregon
- Finalized the IT risk criteria for the potential impact and likelihood of the identified IT risks
- Prioritized the IT risks based on the impact and likelihood criteria
- Developed a proposed three year IT audit plan based on the IT risk assessment results

IV. Reporting

- Documented results of the IT risk assessment
- Reviewed results with Office of Internal Audit and Oregon's senior leadership
- Presented results to senior leadership and the Executive and Audit Committee of the Board of Trustees

IT Units

Baker Tilly identified 27 IT units operating at Oregon, 11 more units than originally identified at the beginning of the assessment. Each of these IT units provides IT services to their own functional area, and many provide IT services to other functional areas across the institution. The IT units identified were:

- Academic Extension
- Athletics
- Business Affairs
- Campus Operations
- Center for Media and Educational Technologies (CMET)
- College of Arts and Sciences (CAS)
- College of Arts and Sciences (CAS) Dean's Office
- College of Education
- Department of Computer and Information Science (CIS)
- Department of Psychology
- Division of Student Life
- Early Childhood (EC) Cares
- Education and Community Support (ECS)
- Enrollment Management
- Finance and Administration
- Housing
- Information Services
- Lundquist College of Business
- Research and Innovation
- School of Architecture and Allied Arts (AAA)
- School of Journalism and Communication (SOJC)
- School of Law
- School of Music and Dance (SOMD)
- University Advancement
- University Health Center
- UO Libraries
- UO Police

Noted Strengths

Over the course of the assessment, Baker Tilly noted the following strengths within Oregon's IT environment:

- Investment in data center infrastructure to provide adequate secure physical space, appropriate cooling systems, redundant battery and power sources, and monitoring services at the Computing Center and Allen Hall data centers
- Virtual machine environments housed in the Computing Center data center, created by both Information Services and the College of Arts and Science's IT unit, to maximize server hardware and provide cost effective platforms available for use by all IT units
- Recent creation of an information security office and hiring of a chief information security officer to develop policies, processes, and practices for securing the University's systems and data
- Many long serving IT professionals within IT units who bring institutional knowledge and expertise that is critical to maintaining the availability and functionality of IT services and systems across campus

Themes

Since Oregon's current model for delivering IT services to the institution is decentralized, we have noted three IT risk themes that transcend IT units and could affect many of the IT risk areas identified. While these themes are not risks, leadership should keep these factors in mind as they address the identified risk areas with new and updated risk management practices.

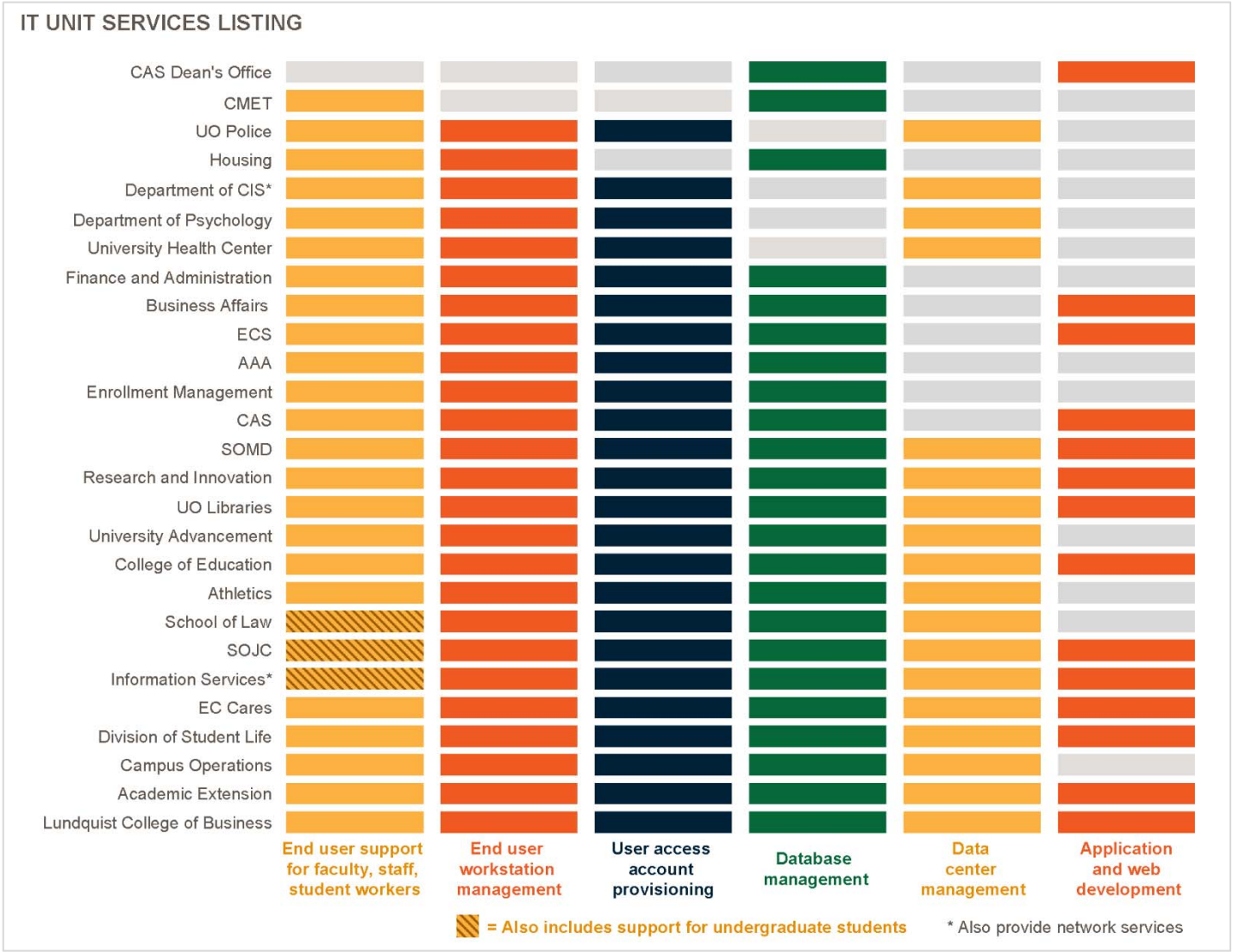
Theme #1: Distribution of IT Services and Collaboration of IT Units

IT services are delivered to faculty, staff, students, and other University community members by all 27 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).

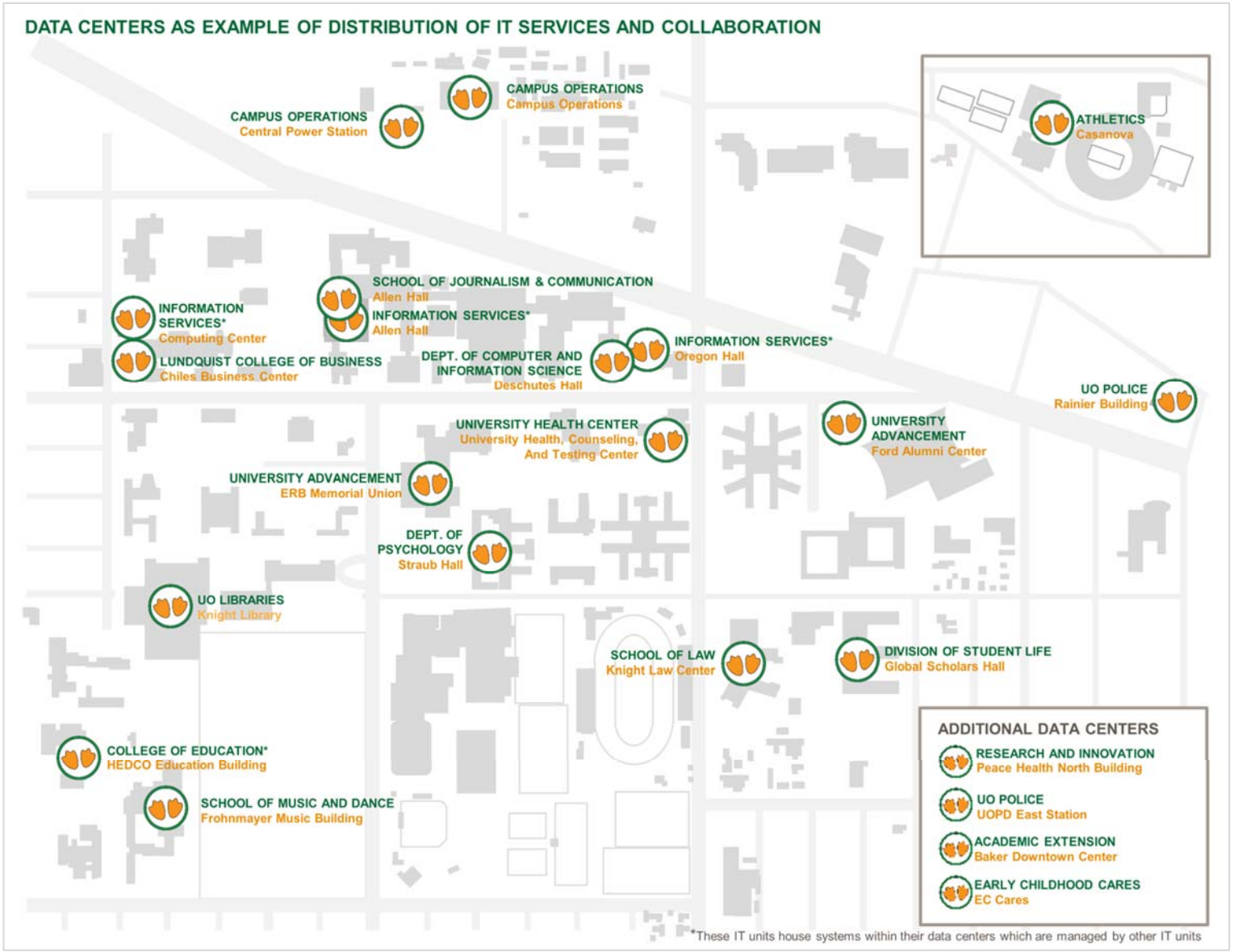
To show the distribution of IT services across units, we have documented in the figure at right the services provided by each IT unit.

In addition to the distribution of IT services across the IT units at Oregon, 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.



As an example of the distribution of IT services and collaboration of IT units, we have documented in the figure at right the various data center facilities (e.g., distinct physical spaces housing servers) that exist across the institution. IT units such as Information Services, College of Education, College of Arts and Sciences, Advancement, UO Police, and Student Life all provide data center services, such as housing systems of others, to functional areas outside of their own functional areas.

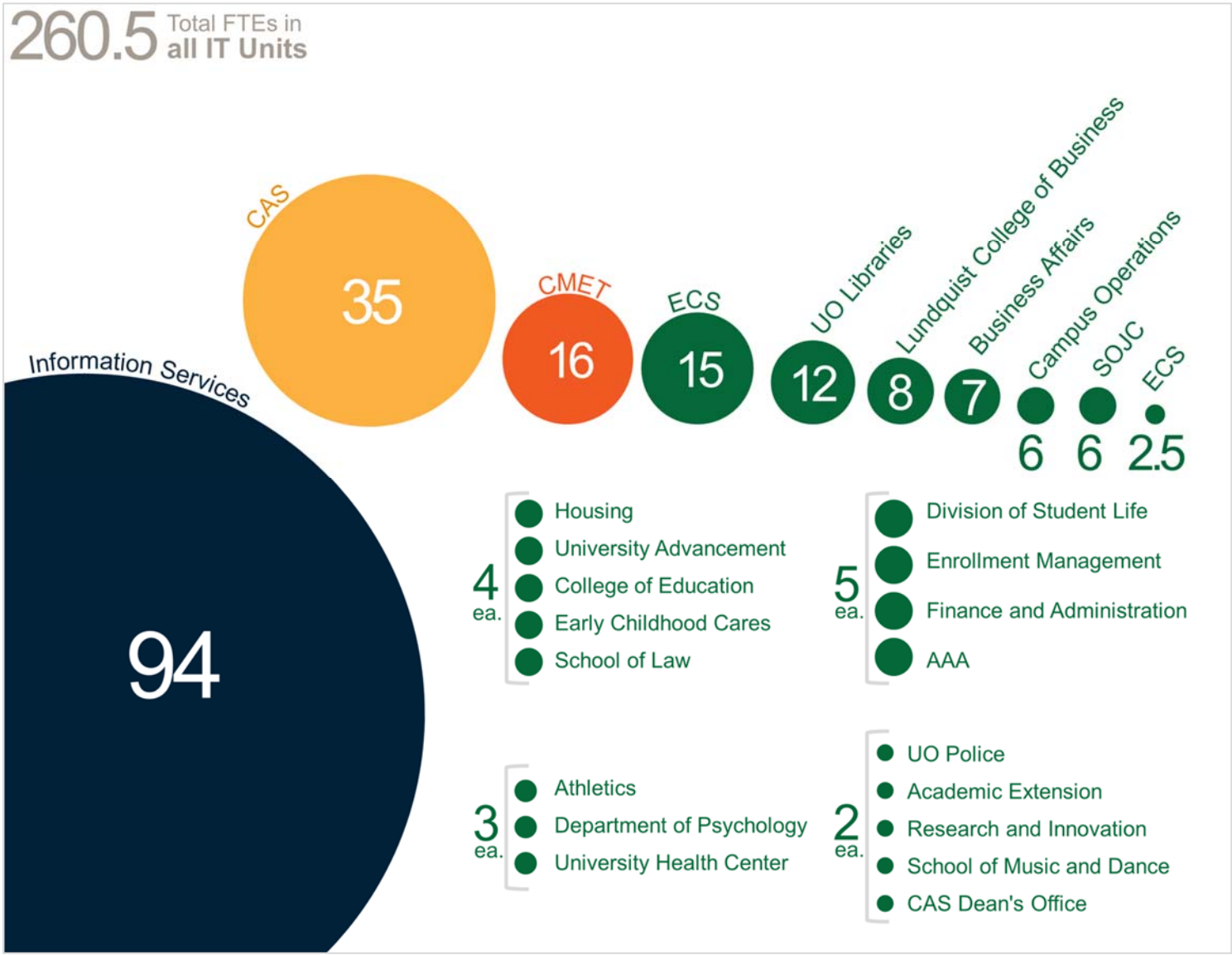


Theme #2: Optimization of IT Resources

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 27 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.

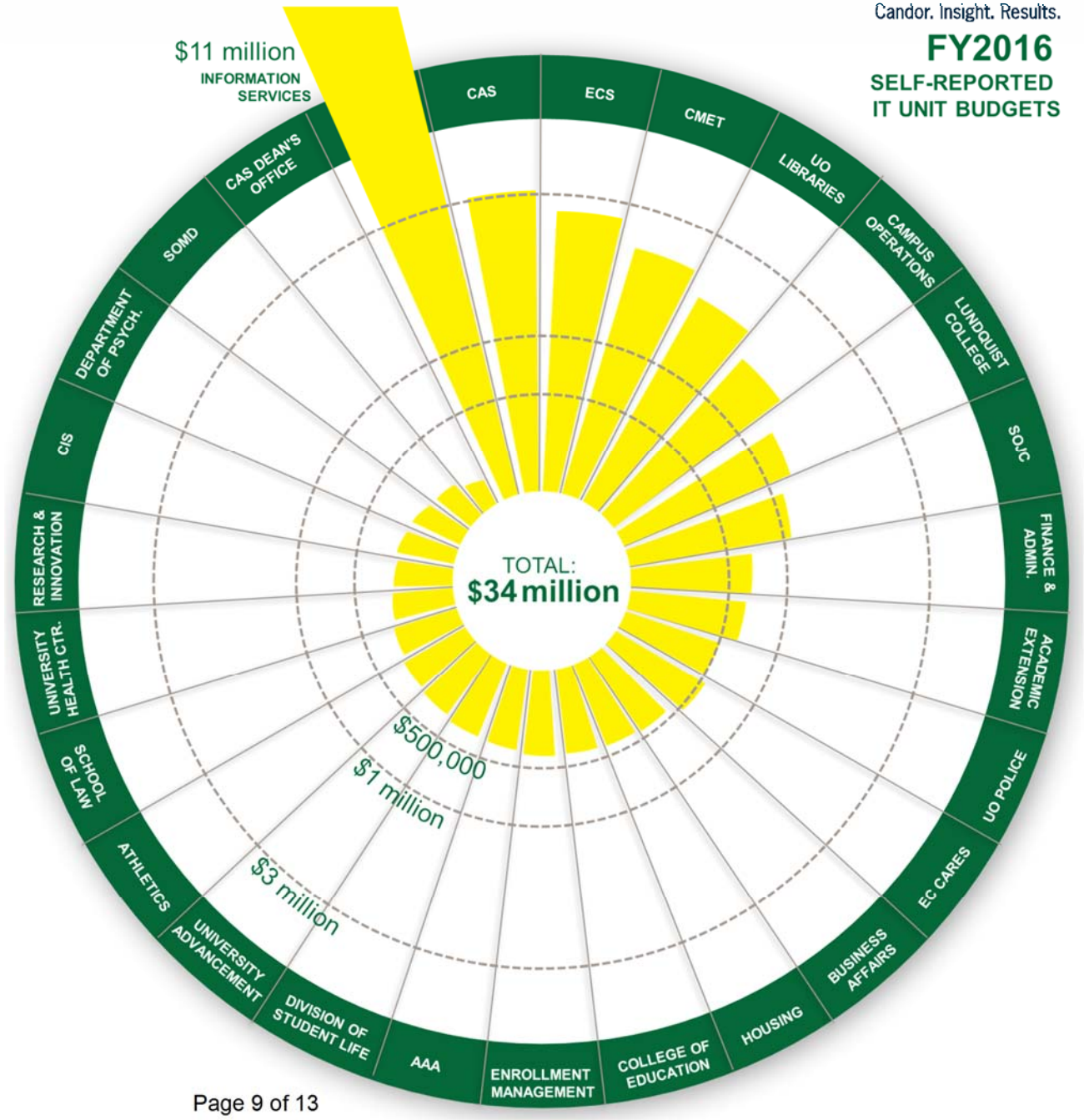
To show the level of decentralization of people resources currently deployed, we have documented in the figure at right the self-reported current full time equivalent (FTE) positions, both staffed and open, in each IT unit.



BAKER TILLY

Candor. Insight. Results.

To show the size of IT budgets across the institution, we have documented in the figure at right the self-reported fiscal year 2016 IT unit budgets (including costs such as salary, hardware, software, and services).

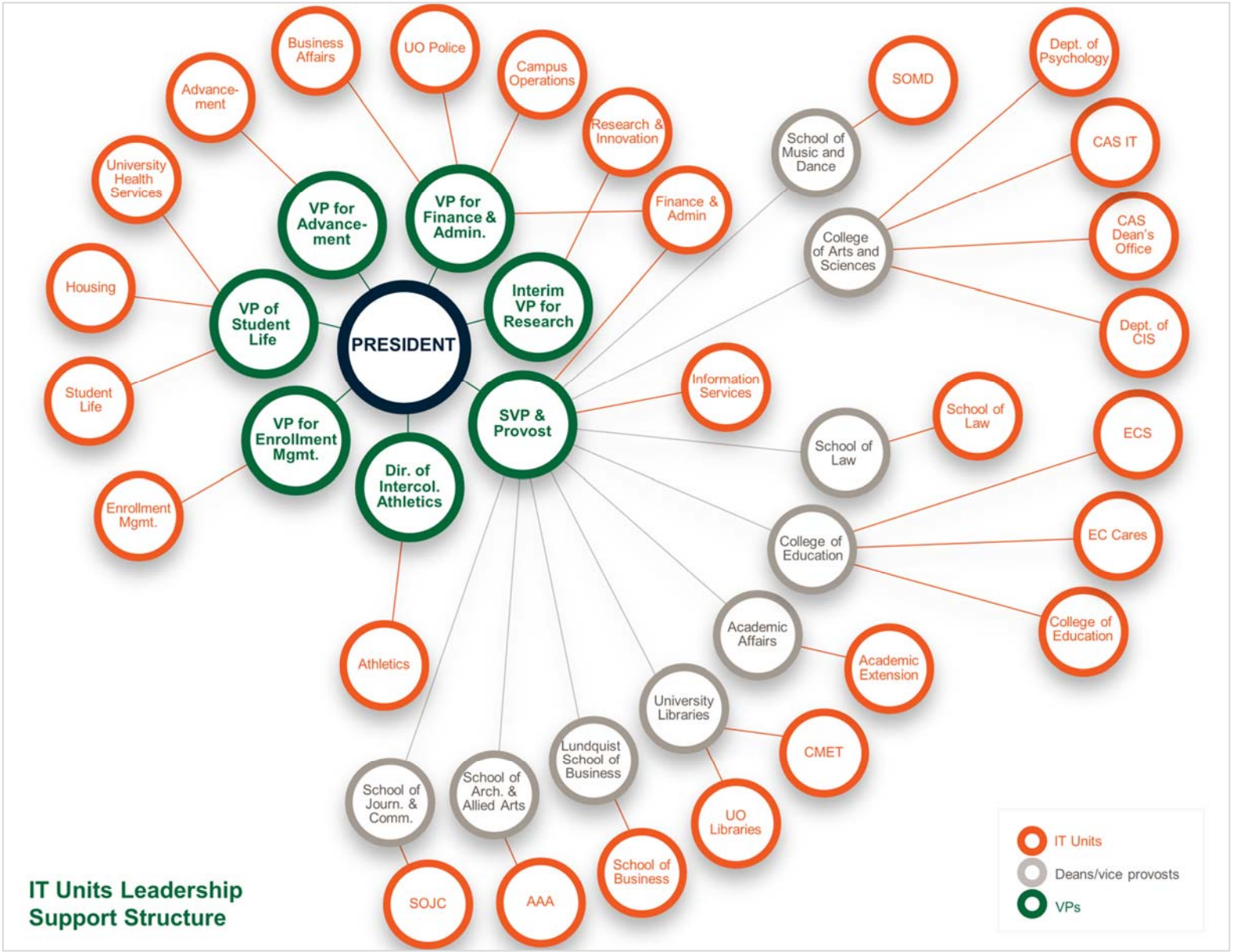


Theme #3: Leadership Support of IT

With the distribution of IT units across the various academic and administrative functions of the institution, the leadership support for IT is dispersed among various vice presidents, deans, and provosts.

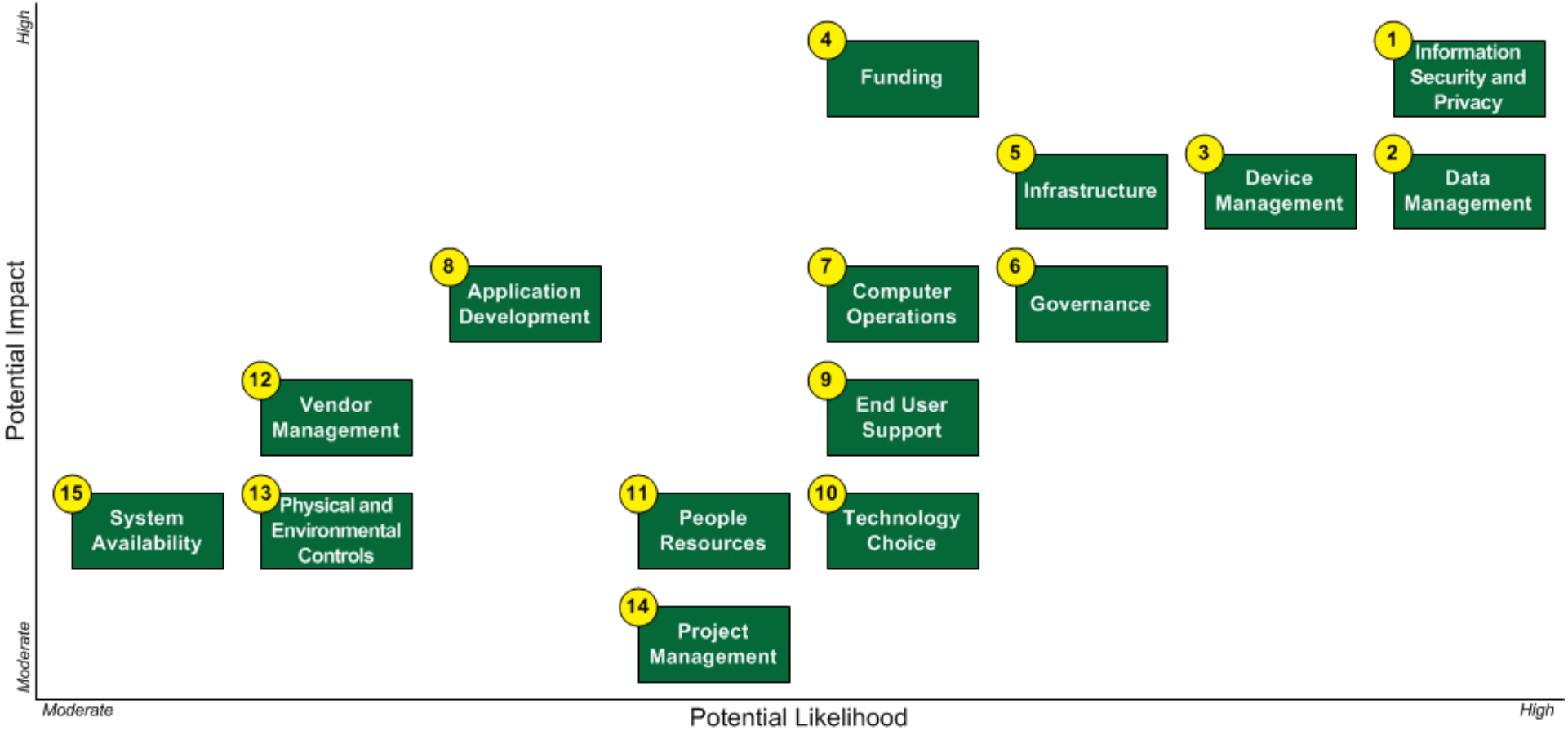
As such, this current structure could make it difficult to address and implement IT risk management strategies consistently and optimize resources across all IT units.

To show this structure, the organization chart at right lists all 27 IT units (in orange) under the functional area of the University to which the IT unit reports. The Provost's office has the most IT units, including the two largest IT units: Information Services and CAS IT.



IT Risks

Oregon 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 Oregon prioritized by the potential impact and likelihood. The placement of the risks on the risk map was based on criteria tailored to Oregon for potential impact and likelihood. The rating of risks was based on judgment, and the criteria were purposely not weighted equally or applied uniformly across the risk areas. Impact was based on reputational, financial, operational, and compliance factors, while likelihood was based on potential timing of occurrence in the short, medium, or long timeframe. The descriptions of each area are listed on the following pages. It is important to note that these areas do not necessarily represent problems, but are risks inherent to Oregon's operations and the environment in which it operates.



IT Risks Descriptions

Baker Tilly identified and prioritized the 15 risk areas specific to Oregon, based on the results of our fieldwork and analysis. Each risk area is described below:

1. **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.

2. **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.

3. **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.

4. **Funding** – The monetary resources allocated to acquire, maintain, and retain the people and technology resources required to operate and manage University systems.

5. **Infrastructure** – The server and network hardware resources used to provide platforms for applications and databases, as well as connectivity within the University and to external resources.

6. **Governance** – The processes and structure for planning, implementing, communicating, and monitoring of IT strategy to meet the University's mission and goals.

7. **Computer Operations** – The policies, practices, and tools implemented to plan, implement, operate, change, and monitor University networks and servers.

8. **Application Development** – The processes and tools used to acquire, build, test, and maintain software applications.

9. **End User Support** – The processes and tools used to provide constituents with help desk support functions and training for University systems.

10. **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.

11. **People Resources** – The personnel resources, both employed and contracted, that provide IT services to various constituencies within and outside of the University.

12. **Vendor Management** – The policies, practices, and tools implemented to identify, contract, procure, and manage third-party IT service and product vendors.

13. **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).

14. **Project Management** – The processes and tools implemented for planning, managing, and reporting on IT projects to ensure a successful outcome.

15. **System Availability** – The policies, practices, and tools implemented for maintaining the availability of systems during or after impactful events.

Appendix A: Baker Tilly Contact Information

Mike Cullen, CISA, CISSP, CIPP/US
Senior Manager
703-923-8339
mike.cullen@bakertilly.com

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