UNIVERSITY OF OREGON

May 31, 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 consideration of the FY19 audit plan, enterprise risk management, and an update on Transform IT and cybersecurity.

The meeting will occur as follows:

Thursday, June 7, 2018 at 10:30 a.m.
Ford Alumni Center, Giustina Ballroom

The meeting will be webcast, with a link available at 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.

Board of Trustees | Executive and Audit Committee
Public Meeting | June 7, 2018, 10:30 a.m.
Ford Alumni Center | Giustina Ballroom

Convene

- Call to order, roll call
- Approval of March and April 2018 minutes (Action)

1. **Quarterly Audit Report and Consideration of FY19 Audit Plan (Action):** Trisha Burnett, Chief Auditor

2. **Enterprise Risk Management:** Andre Le Duc, Associate Vice President and Chief Resiliency Officer; Leo Howell, Chief Information Security Officer

3. **Transform IT – Implementation update:** Jessie Minton, Vice Provost and Chief Information Officer

Meeting Adjourns

Agenda Item #1

Quarterly Audit Report and Consideration of FY19 Audit Plan

Materials for this section will provided as supplemental materials.

Agenda Item #1

Quarterly Audit Report and Consideration of FY19 Audit Plan

UNIVERSITY OF OREGON

Office of Internal Audit Quarterly Report

June 2018

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. During the previous quarter, the office experienced turnover and one position is currently vacant. As a result, some projects that were in process during the prior quarter are still in process. In addition, Internal Audit finalized two assurance projects. 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 hosted a meeting with Chief Audit Executives (CAE's) from the former OUS schools, and began planning a similar even for Pac-12 CAE's. The intent is to provide a forum for networking, information sharing, and other types of collaboration on a recurring basis. Finally, a partnership with student members of Beta Alpha Psi has been successful and is in the finishing stages for the spring term.

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

Scholarship Award Compliance

Internal Audit performed this audit in April. This project was identified after the FY18 audit plan was approved in June. The objective was to ensure all compliance requirements were met for a departmentally selected recipient of a specific scholarship. No instances of noncompliance were noted.

Research Cybersecurity Compliance

Internal Audit, in collaboration with Baker Tilly, began this project in August. This project was identified after the fiscal year 2018 ("FY18") audit plan was approved in June. The objective was to perform a review of grants with specific cybersecurity requirements to ensure the University is in compliance. No instances of noncompliance were noted.

PROJECTS IN PROGRESS

Nonretaliation Policies
Internal Audit began this project in August. 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. *Estimated completion: July 2018*

Athletics IT Assessment
Internal Audit, in collaboration with Baker Tilly, began this project in February. This project was identified on the approved FY18 audit plan. The objective is to conduct an IT assessment for the Athletics department covering key people, processes, and technology used. This project is currently in the fieldwork phase. *Estimated completion: July 2018*

Cash Handling
Internal Audit began this project in September. This project was rolled over from the fiscal year 2017 approved audit plan to the FY18 approved 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"). This project is currently in the fieldwork phase. *Estimated completion: August 2018*

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

I-9 Compliance
Internal Audit, in collaboration with students from Beta Alpha Psi, began this project in April. 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. This project is currently in the fieldwork phase. *Estimated completion: September 2018*

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 FY18 audit plan included 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 that is being 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.

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.

Follow-Up of Lab Safety Practices
Internal Audit began this project in April. Internal Audit followed up on eight observations and 26 management corrective actions. This project is currently being finalized.

Follow-Up of Printing and Mailing Services
Internal Audit began this project in May. Internal Audit will be following up on 20 observations and 20 management corrective actions. This project is currently in the final planning phase.

There are five follow-up projects scheduled for the upcoming quarter, three of which are in the preliminary planning phase.

HOTLINE SUMMARY

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

Reporting Sources for FY18 Investigative Services	
Campus Direct to Internal Audit	2
3rd Party Hotline	10
Grand Total	**12**

It is common for a university our size to have an active hotline. Peer institution benchmarking indicates the activity is low for our institution. 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

In addition to the initiatives described in the summary, and to provide a foundation for the direction of the office, Internal Audit created a strategic plan. Through this process, the mission was updated, and a vision and specific goals were incorporated. Administrative items, such as outreach on campus and involvement in national organizations, were included as goals and specific action items to achieve these goals were included within the plan. An implementation schedule was developed to ensure the strategic plan was achieved. At this time, all action items are on schedule.

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

Resolution: Adoption of FY19 Risk Assessment and Audit Plan

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

Whereas, the University takes seriously the responsibility to manage, invest, and spend resources;

Whereas, the University's Office of Internal Audit (Internal Audit) provides independent, objective evaluations and advisory services that add to the accountability of the University;

Whereas, the Internal Audit works closely with university leadership, faculty, and staff to conduct and coordinate a broad range of audit functions for the University;

Whereas, the Office of Internal Audit has developed an Risk Assessment and Audit Plan for Fiscal Year 2019, attached hereto as Exhibit A; and,

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

NOW, THEREFORE, the Executive and Audit Committee of the Board of Trustees of the University of Oregon hereby approves the proposed FY18 risk assessment audit plan attached hereto and directs the officers, or their designee(s), of the University to take all actions and steps deemed necessary and proper to implement the approved plan.

Moved: _____ Seconded: _____

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

Dated: _____ Recorded: _____

EXHIBIT A

Office of Internal Audit
Annual Risk Assessment and
Internal Audit Plan

FY2019

Risk Assessment
Conducted for the purpose of developing the
Annual Risk Based Audit Plan

TABLE OF CONTENTS

EXECUTIVE SUMMARY

During FY18, the Office of Internal Audit (Internal Audit) refined the risk assessment methodology to ensure the annual audit plan was appropriately determined. During the process, the method to identify risk included more input from the campus community and peer institutions. Using the results of this process, Internal Audit has created the FY19 audit plan.

Time will also be allocated on the audit plan for consulting services and administrative tasks. Internal Audit will advise on internal controls, compliance, efficiency, and effectiveness in any areas requested by management. Internal Audit will also use administrative time to research process improvements, implement strategic plan goals, and continue mentoring students working with the office. The progress and action plans will be included in communications to the Board of Trustees.

METHODOLOGY

During the preparation of the FY19 audit plan, Internal Audit used a comprehensive risk assessment process to ensure appropriate coverage. Internal Audit used five (5) different risk sources defined as follows:

1. Risk Source #1: Central Control Functions
2. Risk Source #2: Interviews
3. Risk Source #3: SERMC Risk Matrix
4. Risk Source #4: Survey
5. Risk Source #5: Miscellaneous

Risk Source #1 – As Internal Audit builds the annual audit plan, one focus continues to be validating fundamental control systems, including evaluation of administrative oversight functions. As the plan is prepared each year, these areas will be considered for coverage and ideally be placed on a rotation. Audit objectives will focus on evaluating the internal control structure of oversight functions based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model and the efficiency of processes.

Risk Source #2 – Interviews were held with members of senior leadership and others in key positions to gather information about factors that could prevent the university from meeting its objectives.

Risk Source #3 – The results of the SERMC Risk Matrix identifies risks that could negatively affect the university's ability to achieve its core mission of instruction, research, and public service. As a result of this process, leadership identifies areas of focus for the coming year.

Risk Source #4 –An anonymous survey was sent to the campus community to gather input. The responses were reviewed and any auditable topics identified were included in the risk assessment.

Risk Source #5 – Miscellaneous sources, such as information noted by Internal Audit during previous work, financial impact of the unit, and the last time the unit was audited. In addition, information from other institutions, or nationwide trends/issues in higher education were considered.

Using this criteria, risk rank was assigned based on the audit staff's best judgment considering the likelihood of the event occurring and impact to the institution.

RESULTS

Vision Statement
To be a premier partner that adds value, provides objective insight, and proactively collaborates to maintain the highest standard of excellence.

Mission Statement
Driven by the highest professional an ethical standards, 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.

Introduction
The Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF) requires the chief audit executive to establish a risk-based plan to determine the priorities of the internal audit function.

Audit Resources
Internal Audit is currently comprised of a chief auditor, a senior auditor, and an associate auditor. Hiring for a vacant internal auditor position is expected to take place by September. Student time is also expected to be utilized, however cannot be easily determined. Audit staff resources are expected to be allocated as follows:

Position	Gross Available Hours		Leave & Holidays	Training & Related Travel		Other Administrative Tasks		Net Available Hours
Chief Auditor	2,080		350	75		720		935
Senior Auditor	2,080		350	75		415		1,240
Associate Auditor	2,080		350	75		665	*	990
Internal Auditor	1,730	#	350	140	^	240		1,000
Total	7,970		1,400	365		2040		4,165

* Note this position is 40% executive support

Expected hire date September 1, 2018

^ Note that in addition to annual continuing education requirements, new employees are required to attend University orientation and other introductory trainings.

2019 Audit Plan
Internal Audit has identified an audit plan incorporating high-risk areas based on several sources, as well as including the validation of central control functions. These high-risk areas are shown as planned audit projects (Tier 1) below. Other risks were identified through the risk assessment process and considered to be high probability, but low overall impact to the University. These projects have been identified as Tier 2 and are reserved for student mentoring projects. Other administrative goals for FY19 include, but not limited to, process improvements, strategic plan initiatives, and student mentoring.

Internal Audit engages in three primary activities – assurance, consulting, and investigative services. Additionally, Internal Audit performs follow-up engagements and coordinates external audit efforts. The focus of Internal Audit is to actively work with the university to assist management in addressing strategic, financial, operational, compliance, and reputational risk and exposures on both university-wide and departmental level processes and control systems. Internal Audit brings a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal Audit's planned audit projects (Tier 1) for FY19 are:

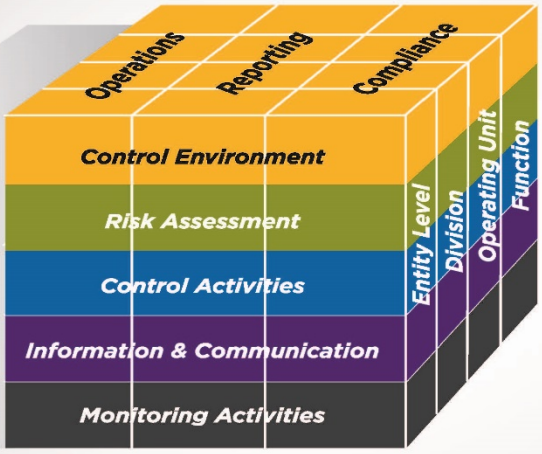
Audit Unit	Audit Title	Audit Focus	Risk Source	Estimated Hours
Assurance Services				
Projects in progress from FY18 Plan	Various	Various	FY18	370
Athletics	NCAA Compliance Program	To evaluate the effectiveness of the program using a compliance framework	Rollover from FY18	200
University Wide	Inventory of Critical Business Functions	To perform an assessment of where and how decentralized critical business processes occur at the University.	1,2,4,5	1000
International Affairs	International Student Employment	To assess compliance with DHS and other relevant requirements for international student employment.	1,2,3,5	200
University Health Center	Health Center IT Assessment	To conduct an IT assessment for the Health Center IT department covering key people, processes, and technology	2,3	100
Business Affairs Office	Payment Card Industry (PCI) Program Assessment	To review and assess the University's program for complying with PCI Data Security Standards (DSS) requirements.	1,2,3	40
Student Financial Aid	GLBA Financial Assistance Compliance	To assess how the University's financial aid processes meet the GLBA requirements outlined in the 2016 Dear Colleague Letter.	2,5	40
Athletics	Ticket and Parking Sales Processes	To evaluate the adequacy of controls over reporting and accountability for ticket and parking sales	5	200
Athletics	Athletic Equipment	To determine if Athletic equipment is appropriately safeguarded, tracked, and in compliance with NCAA and financial reporting obligations.	5	160
UOPD	Firearms Inventory	To verify that all firearms purchased by the UOPD are tracked, accounted for, and properly registered as required.	5	120
Athletics	Ticket Count	To verify average minimum attendance per the NCAA Division I requirements.	Required	60
College of Education	Scholarship Verification	To verify that the selected awardee meets the qualifications as listed in the award agreement.	5	10
Consulting Services				
Campus Wide	Trainings and Presentations	Internal Audit will continue offering training on internal controls, risk, and fraud awareness as requested and plans to establish ongoing		85

		professional development opportunities.		
Campus Wide	Consulting Services	Management may ask Internal Audit for advisory services to be performed in accordance with the mission and authority of Internal Audit.		350
Campus Wide	Facilitated Internal Control Self Assessments	Solicit areas of the campus to participate in facilitated internal control self-assessments.		100
Investigative Services				
Campus Wide	Investigative Audits	Based upon the number of reports received from Ethics Point hotline and management.		300
Follow-Up				
Campus Wide	Follow up procedures	Follow up on corrective actions from previous engagements.		500
External Audit Coordination				
Business Affairs, Sponsored Projects Services & Athletics	Financial Statements, Single Audit, and NCAA AUP	Coordinate with and provide oversight of external audit in accordance with the Internal Audit Charter.		80
Risk Assessment & Audit Planning				
Campus Wide	Annual Risk Assessment	The annual risk assessment forms the basis of the audit planning for future years. Estimated budget includes participation in and alignment with Enterprise Risk Services enterprise wide risk assessment.		250
			Total Hours	4165

Internal Audit's Tier 2 audit projects for FY19 are:

Audit Unit	Audit Title	Audit Focus	Risk Source	Estimated Hours
Business Affairs Office/Various Units	Personal Reimbursements	To verify employee reimbursements were appropriate and evaluate internal controls around reimbursements.	1,2,5	N/A
Business Affairs Office/Various Units	Journal Vouchers	To verify journal vouchers posted by employees were appropriate and evaluate internal controls around journal vouchers.	1,2,5	N/A
Business Affairs Office/Various Units	System Access Review	To verify system access is appropriate based on review of employee job responsibilities, including ensuring segregation of duties is maintained.	1,2,5	N/A
Business Affairs Office/Purchasing and Contracting Services/Various Units	Vendor Reviews	To verify appropriate contracts are in place, as required.	1,2,5	N/A
Purchasing and Contracting Services/Various Units	Purchasing Cards (P-cards)	To verify P-card purchases were appropriate and evaluate the internal controls around P-card purchases.	1,2,5	N/A
University-Wide	Affiliated Entities	To gain an understanding of entities affiliated with the University and ensure appropriate MOU's are in place.	2,5	N/A

COSO Internal Control — Integrated Framework Principles



Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly affect the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

For more information about COSO, visit coso.org.

The Board of Trustees is involved in exercising oversight for the development and performance of internal control through each of the five components of the *Framework,* as illustrated in the table below:

Internal Control Component	Oversight Activities of the Board
Control Environment	• Oversee the definition of and apply the standards of conduct of the University • Establish the expectations and evaluate the performance, integrity, and ethical values of the President • Establish oversight structures and processes aligned with the objectives of the University (e.g., Board and committees as appropriate with requisite skills and expertise) • Commission Board oversight effectiveness reviews and address opportunities for improvement • Exercise fiduciary responsibilities and due care in oversight (e.g., prepare for and attend meetings, review the University's financial statements and other disclosures) • Challenge senior management by asking probing questions about the University's plans and performance, and require follow-up and corrective actions, as necessary (e.g., questioning transactions that occur repeatedly at the end of interim or annual reporting periods)
Risk Assessment	• Consider internal and external factors that pose significant risks to the achievement of objectives; identify issues and trends (e.g., sustainability implications of the University's operations) • Challenge management's assessment of risks to the achievement of objectives, including the potential impact of significant changes (e.g., risks associated with entering a new market), and fraud or corruption • Evaluate how proactively the University assesses risks relating to innovations and changes such as those triggered by new technology or economic and geopolitical shifts
Control Activities	• Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary (e.g., in response to significant risks emerging from internal or external factors) • Oversee senior management in its performance of control activities
Information and Communication	• Communicate direction and tone at the top • Obtain, review, and discuss information relating to the University's achievement of objectives • Scrutinize information provided and present alternative views • Review any financial statement disclosures for completeness, relevance, and accuracy • Allow for and address upward communication issues
Monitoring	• Assess and oversee the nature and scope of monitoring activities, any management overrides of controls, and management's evaluation and remediation of deficiencies • Engage with management, internal and external auditors, and others, as appropriate, to evaluate the level of awareness of the University 's strategies, specified objectives, risks, and control implications associated with evolving business, infrastructure, regulations, and other factors

Transparency obligations reinforce accountability of both senior management and the Board of Trustees. The Board of Trustees oversees such that needs are understood and met over time. Reporting to the Board of Trustees occurs both on a regular and ad hoc basis, as needed, to help the Board oversee the issues relating to the system of internal control.

Agenda Item #2

Enterprise Risk Management

Strategic Enterprise Risk Management and Compliance Committee Update

Date: June 7, 2018

Board of Trustees of the University of Oregon

Presented by:

André Le Duc, Chief Resilience Officer and

Associate Vice President, Safety and Risk Services

Presentation Agenda

- Committee charge and membership
- Work group updates
- 2018 Risk Exposure Quadrant Map
- Cyber security overview

  Leo Howell, Chief Information Security Officer, Information Services

Strategic Enterprise Risk Management and Compliance Committee (SERMC)

Committee charge from the President:

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 communication, problem-solving, and collaboration across divisions, units, and departments

Committee Members

- Vice President, Finance and Administration and Chief Financial Officer
- Vice President for Research and Innovation
- Vice President for Student Life
- Vice President for Student Services and Enrollment Management
- Vice President for University Communications
- Vice President for University Advancement
- Vice President and General Counsel to the University
- Vice President for Equity and Inclusion
- Executive Vice Provost for Operations
- Chief Information Officer and Vice Provost for Information Services
- 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

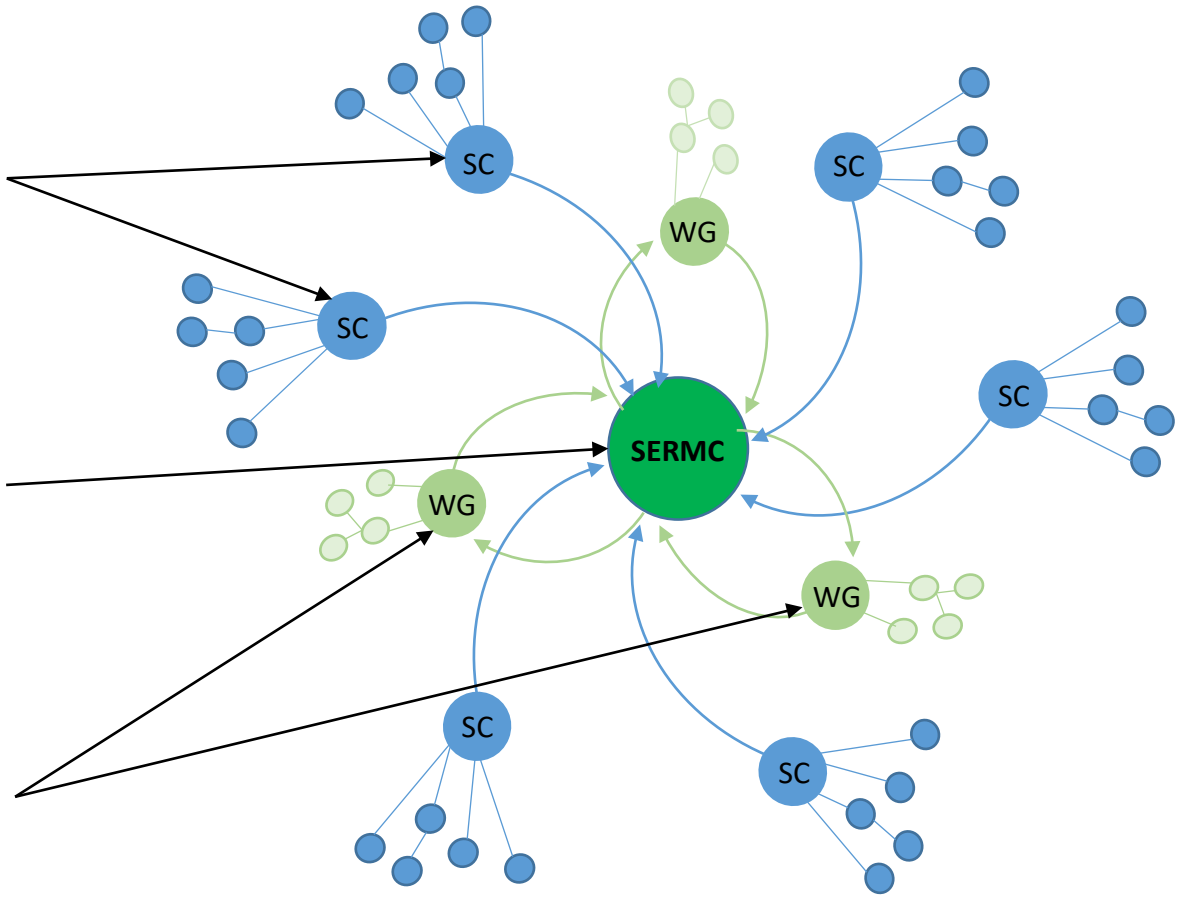
SERMC Network Approach

Link, Align, and Leverage

Standing Committees (SC): UO committees or groups with a charge to address risk or safety

SERMC Committee: Serves as a *"hub"* for leadership to understand exposures, risks, and controls

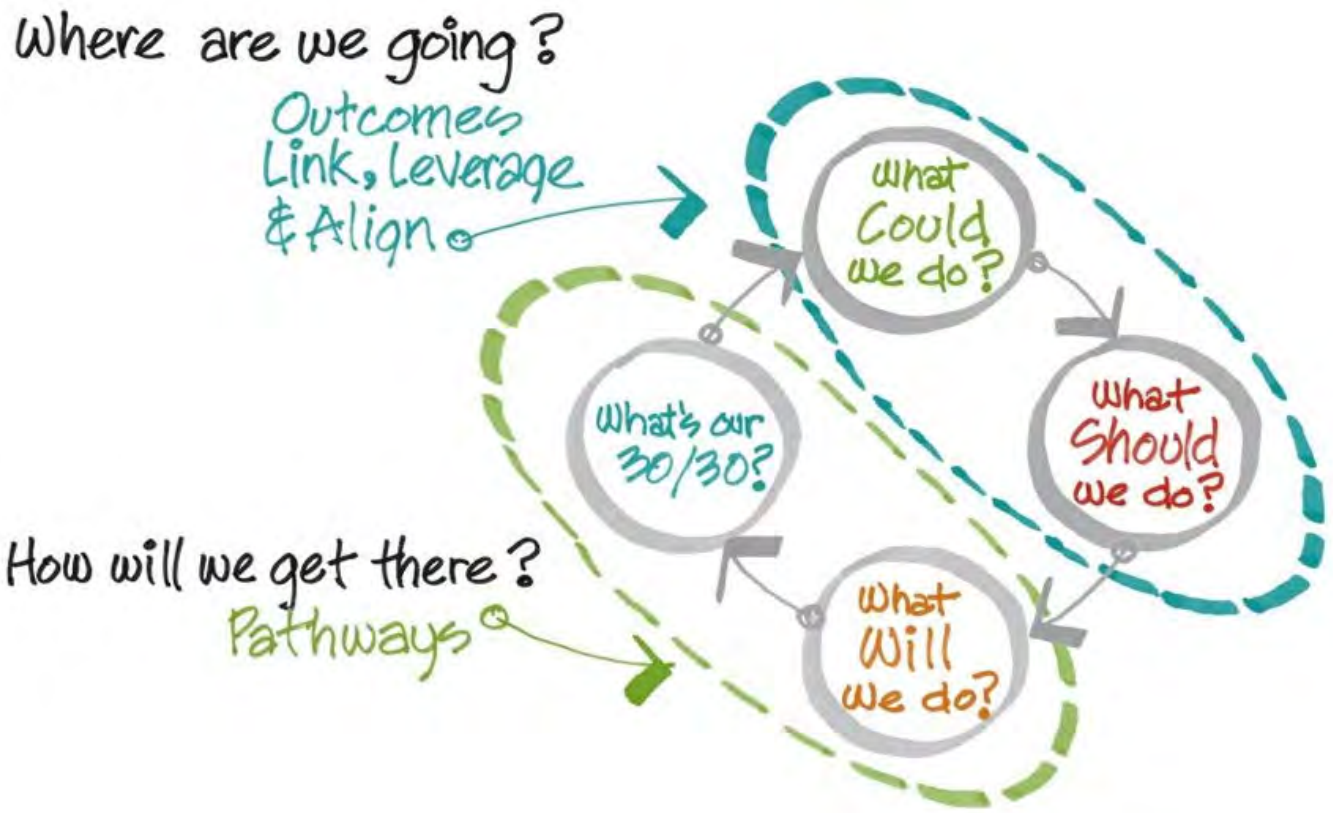
SERMC Work Groups (WG): Topic-specific work groups charged by and reporting to SERMC Committee



Work Group Process

From Risk Identification to Action

Strategic Doing™
Do More Together.



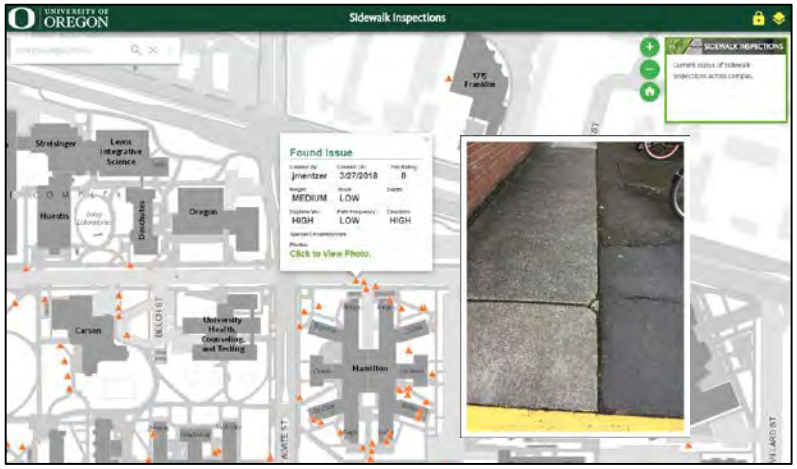
Committee Work Group Updates

COMPLETE:

- Contract Insurance Waivers
- Export Control Laws and Compliance
- Sidewalk Hazard (e.g., slips, trips, and falls) Mitigation

ACTIVE:

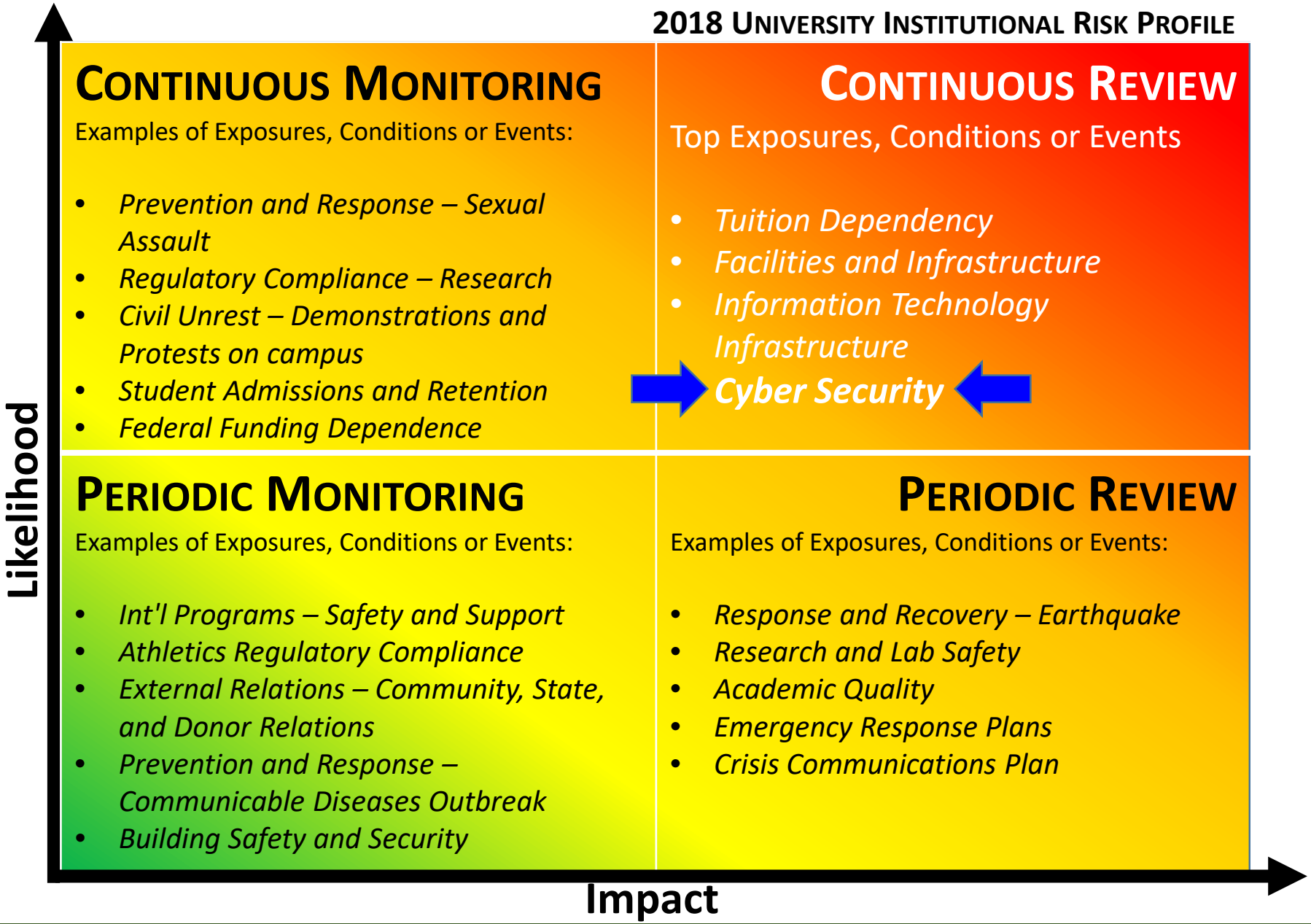
- Business Operations Abroad
- Technology Accessibility
- Enterprise Training Systems
- Nighttime Safety and Violence Prevention



2018 Risk Exposure Quadrant Map

The UO Risk Exposure Quadrant Map is based on the data detailed in the UO Risk Exposure Matrix and provides a high-level summary of conditions, events or exposures that could have an impact on the University's mission and strategic objectives.

2018 University Institutional Risk Profile



Continuous Monitoring

Examples of Exposures, Conditions or Events:

- *Prevention and Response – Sexual Assault*
- *Regulatory Compliance – Research*
- *Civil Unrest – Demonstrations and Protests on campus*
- *Student Admissions and Retention*
- *Federal Funding Dependence*

Continuous Review

Top Exposures, Conditions or Events

- *Tuition Dependency*
- *Facilities and Infrastructure*
- *Information Technology Infrastructure*
- ***Cyber Security***

Periodic Monitoring

Examples of Exposures, Conditions or Events:

- *Int'l Programs – Safety and Support*
- *Athletics Regulatory Compliance*
- *External Relations – Community, State, and Donor Relations*
- *Prevention and Response – Communicable Diseases Outbreak*
- *Building Safety and Security*

Periodic Review

Examples of Exposures, Conditions or Events:

- *Response and Recovery – Earthquake*
- *Research and Lab Safety*
- *Academic Quality*
- *Emergency Response Plans*
- *Crisis Communications Plan*

Cybersecurity Strategic Plan

a sneak preview…

secureU

Key Message

- **IT and Data are pivotal for advances in research,** academics, and services
- Compliance, evolving threats, dependences on IT present opportunities for ***Cybersecurity*** to ***increase our competitive edge***
- This strategy will empower the campus to work together to ***maximize business opportunities, minimize risks, protect individual privacy and security***, and increase alignment with institutional priorities

Ask: recognize cybersecurity as a *competitive benefit*; support the strategic plan

Cybersecurity Business Drivers

External

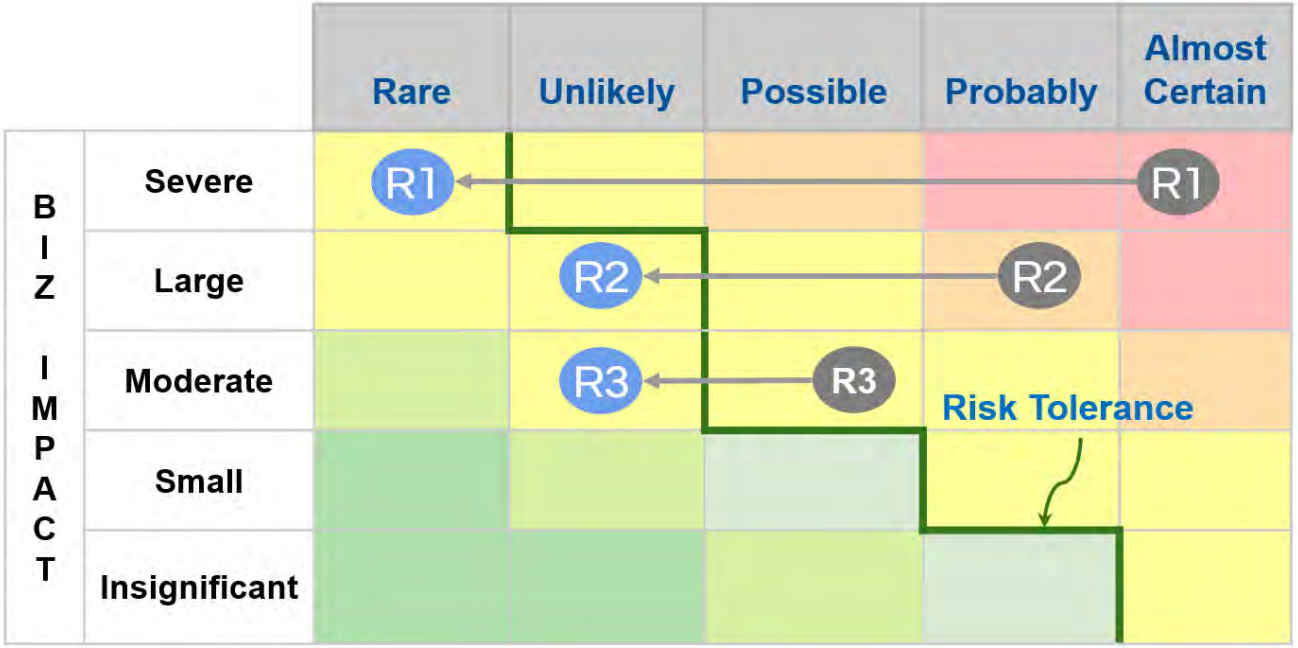
- Regulatory compliance
  DFARs, GLBA, GDPR, HIPAA, DUAs, FERPA…
- Evolving threats
- Social responsibility

Internal

- Advances in Research and Academics
- Enrollment growth
- Dependences on increasingly complex IT

Current Cyber Risk Profile

Minimize Breach, Protect the Brand, Maintain Operations



Legend

Now → future

R1	Data Breach
R2	Loss Business Opportunities
R3	Business Disruption

Threat Landscape

Targeted Assets

Intellectual Property

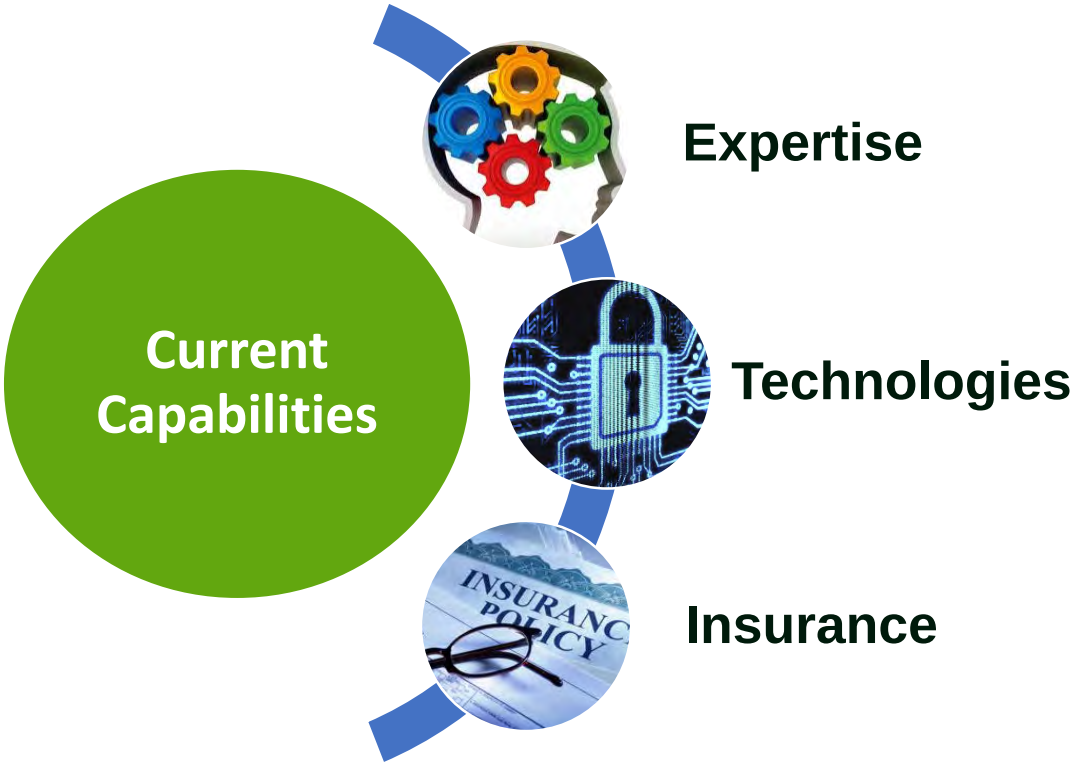
Personally
Identifiable
Information

Adversary

Nation States

Organized Crime

Capabilities & Limitations

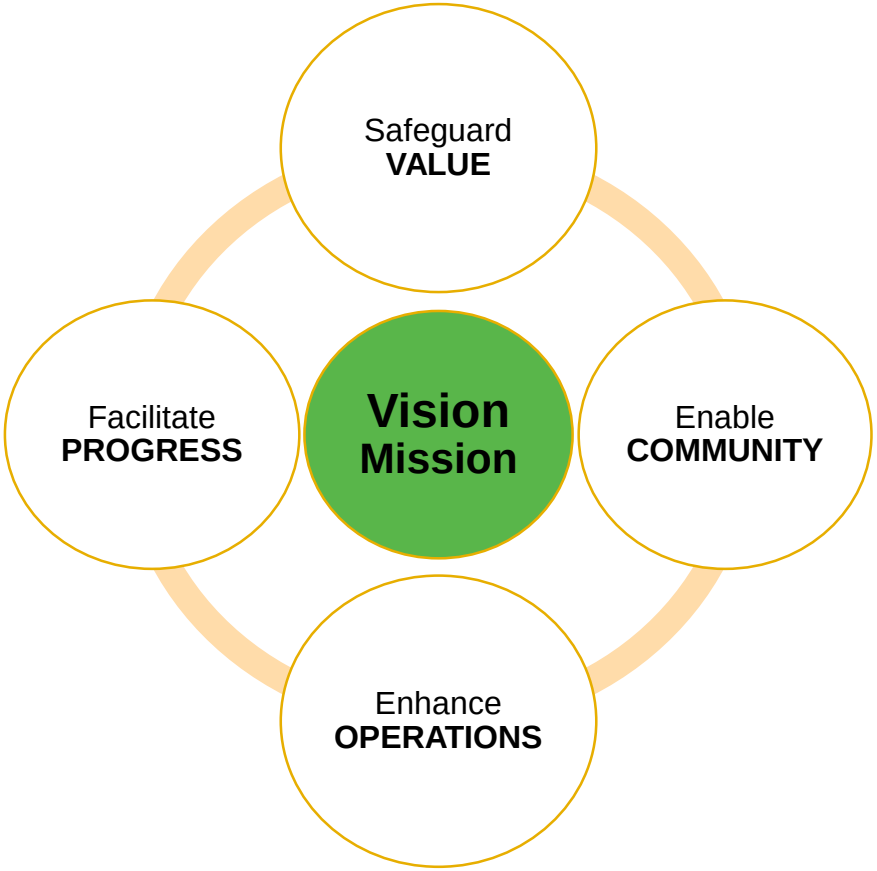


Limitations

- ❑ Resources
- ❑ Coverage
- ❑ Reactive focus
- ❑ Non-compliance

Strategy to ***secureU***

Plan Components



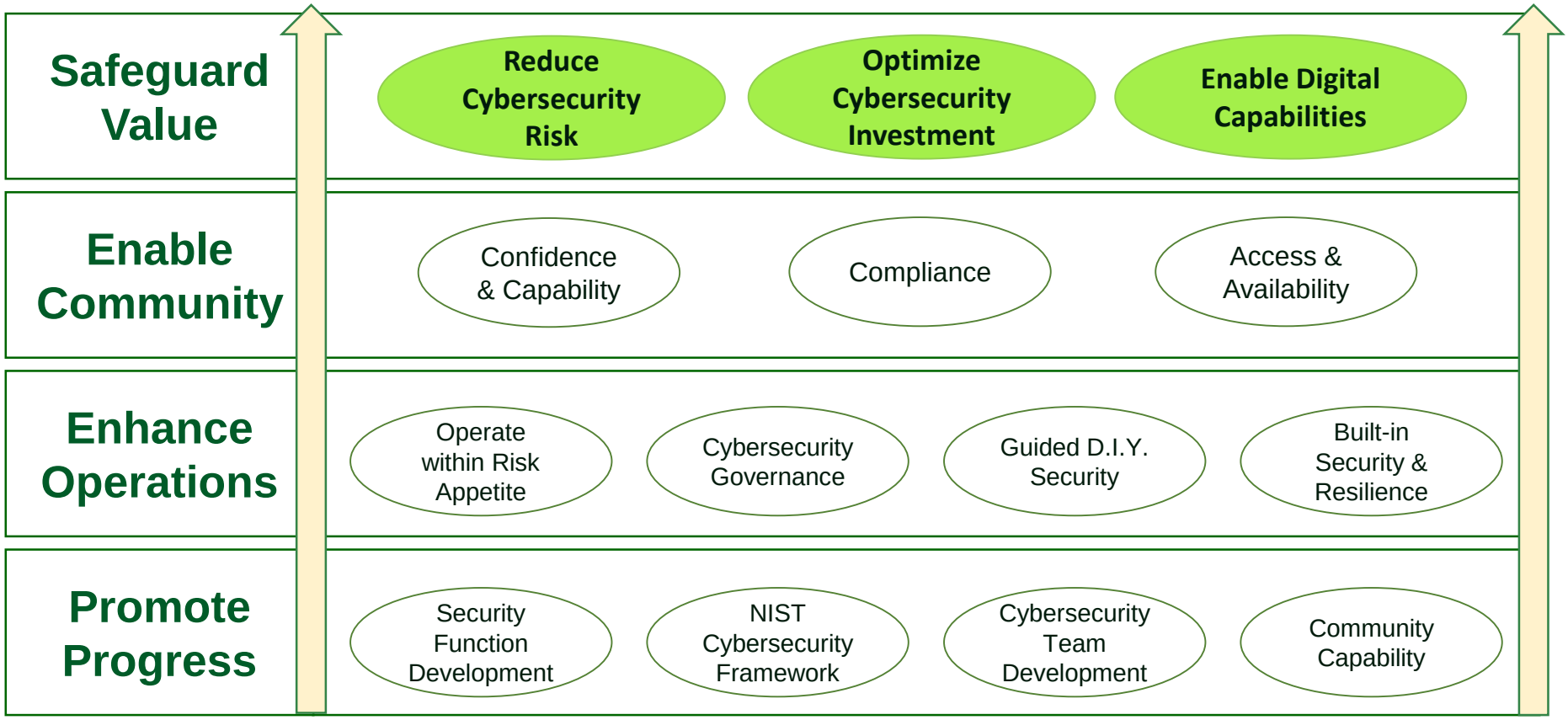
Vision

A knowledgeable and capable UO community working together to safeguard our digital assets and capabilities, while empowering excellence in teaching, research and services in a resilient cyber environment

Mission

To empower the UO community to leverage digital assets and capabilities, while defending our cyber environment from nefarious actors through proactive measures

Cybersecurity Strategy Map



Transition to *secureU*

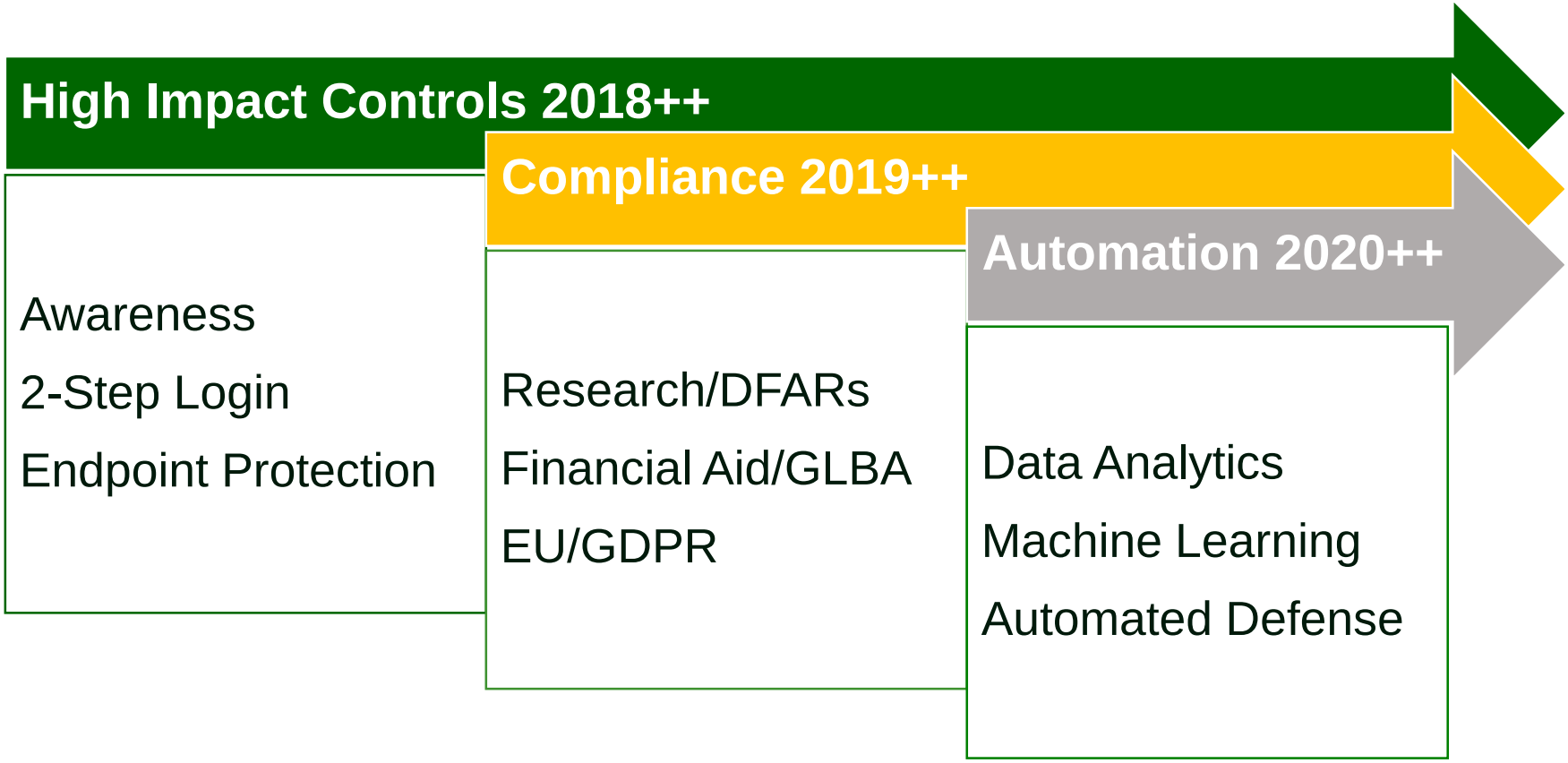
Investments Needed

- Creative staffing
- Cybersecurity automation
- Governance

Benefits

- Maximize business opportunities
- Reduce cyber risks
- Increase business alignment

Implementation Strategy



Key Takeaways

- **IT and Data are pivotal for advances in research,** academics, and services
- Compliance, evolving threats, dependences on IT present opportunities for ***Cybersecurity*** to ***increase our competitive edge***
- This strategy will empower the community to work together to ***maximize business opportunities, minimize risks, protect individual privacy and security***, and increase alignment with institutional priorities

Ask: recognize cybersecurity as a *competitive benefit*; support the strategic plan


RESILIENT™
CREATE A RESILIENT UNIVERSITY–START WITH A RESILIENT YOU

Questions

Agenda Item #3

Transform IT – Implementation Update

UNIVERSITY OF OREGON

Information Technology Update

Date: June 7, 2018

Board of Trustees of the University of Oregon

Presented by:

Jessie Minton, Vice Provost and Chief Information Officer

Information Technology at UO

Vision: UO will strive to create a collaborative and secure IT environment that attracts and retains the best students, faculty, and staff by providing a common foundation of anytime/anywhere technology access for all UO "citizens" and that focuses on strategically funding targeted technology capabilities to support its learning and research goals.

To achieve this, we must:

- Ensure that a collaborative IT governance model is deployed that continually focuses on prioritizing, funding, and driving community-valued IT services
- Recognize that having a secure and robust underlying technology infrastructure is critical to providing all other technology services
- Identify cross-campus core IT services that are more cost-effectively provided in a centralized approach and use the potential savings to fund strategically targeted projects
- Mobilize collaborative cross-campus constituencies to identify and address common goals
- Streamline our administrative processes and systems to provide more seamless and automated service to all campus stakeholders
- Have consistent and strong executive support to ensure that the IT Strategic Plan is supported
- Excite students and faculty to leverage technology to improve learning and research outcomes

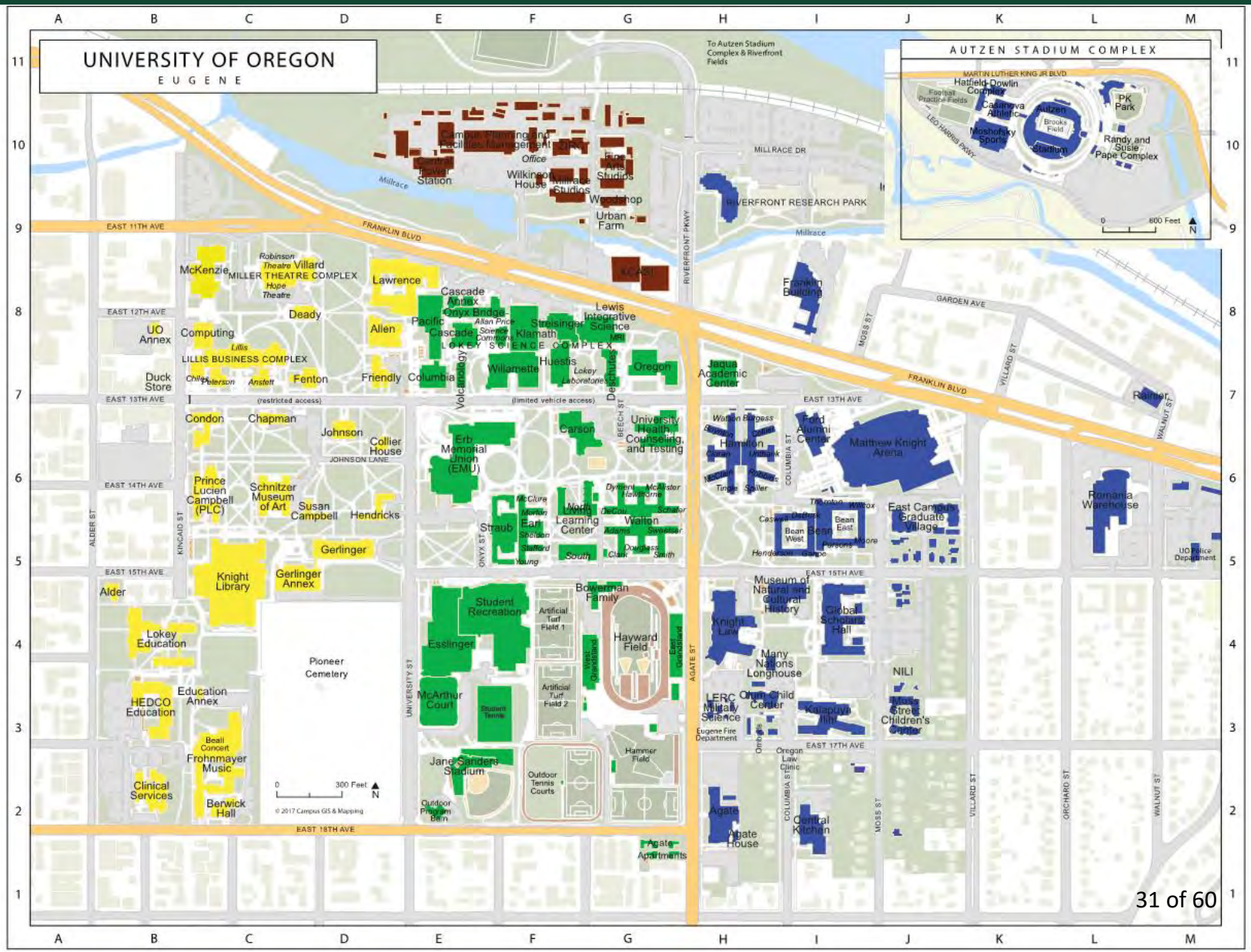
Agenda

- Connectivity
- Governance
- Foundational IT Maturity
- Technology Risks

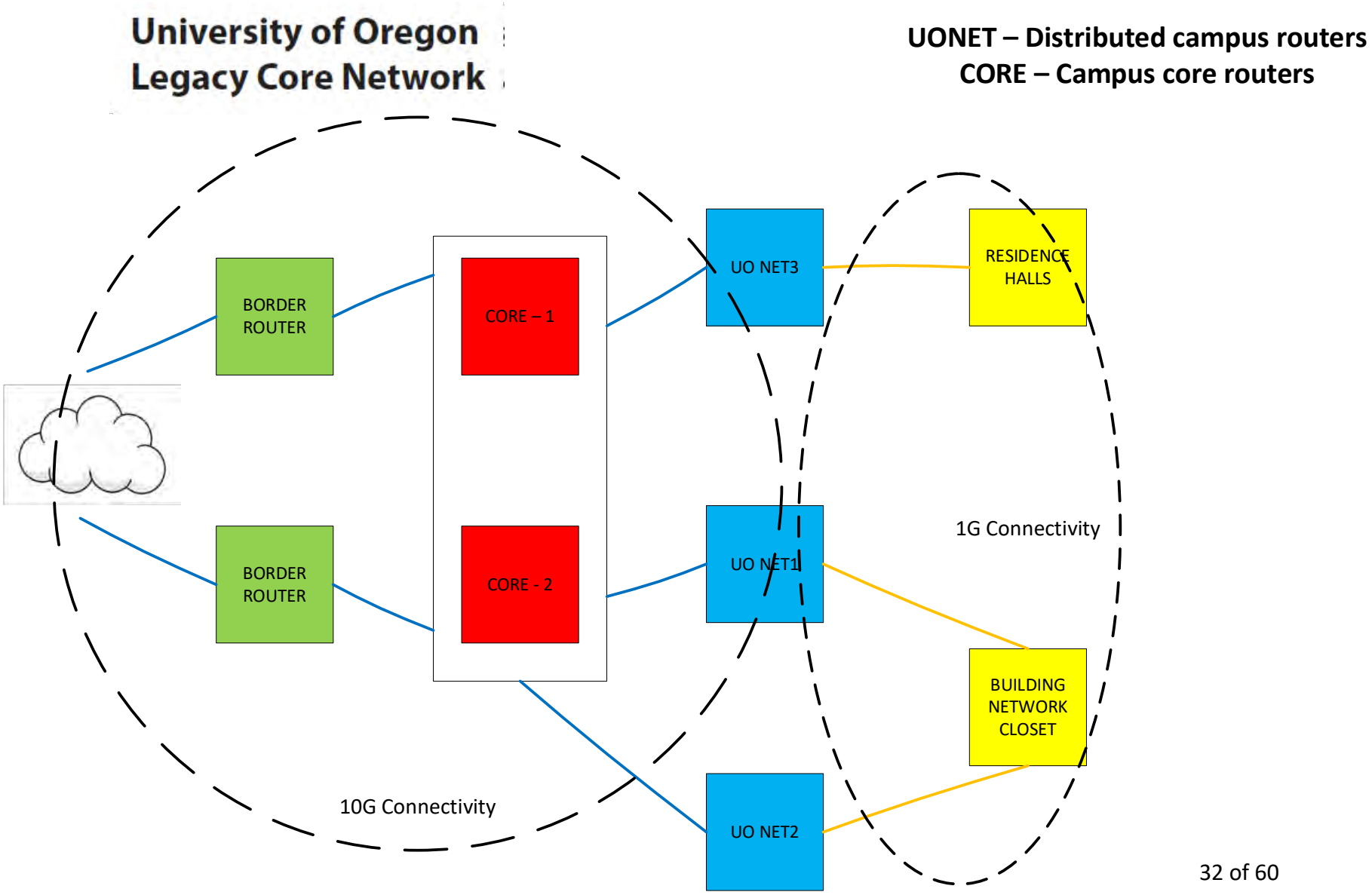
Connectivity

On campus and across the state of Oregon

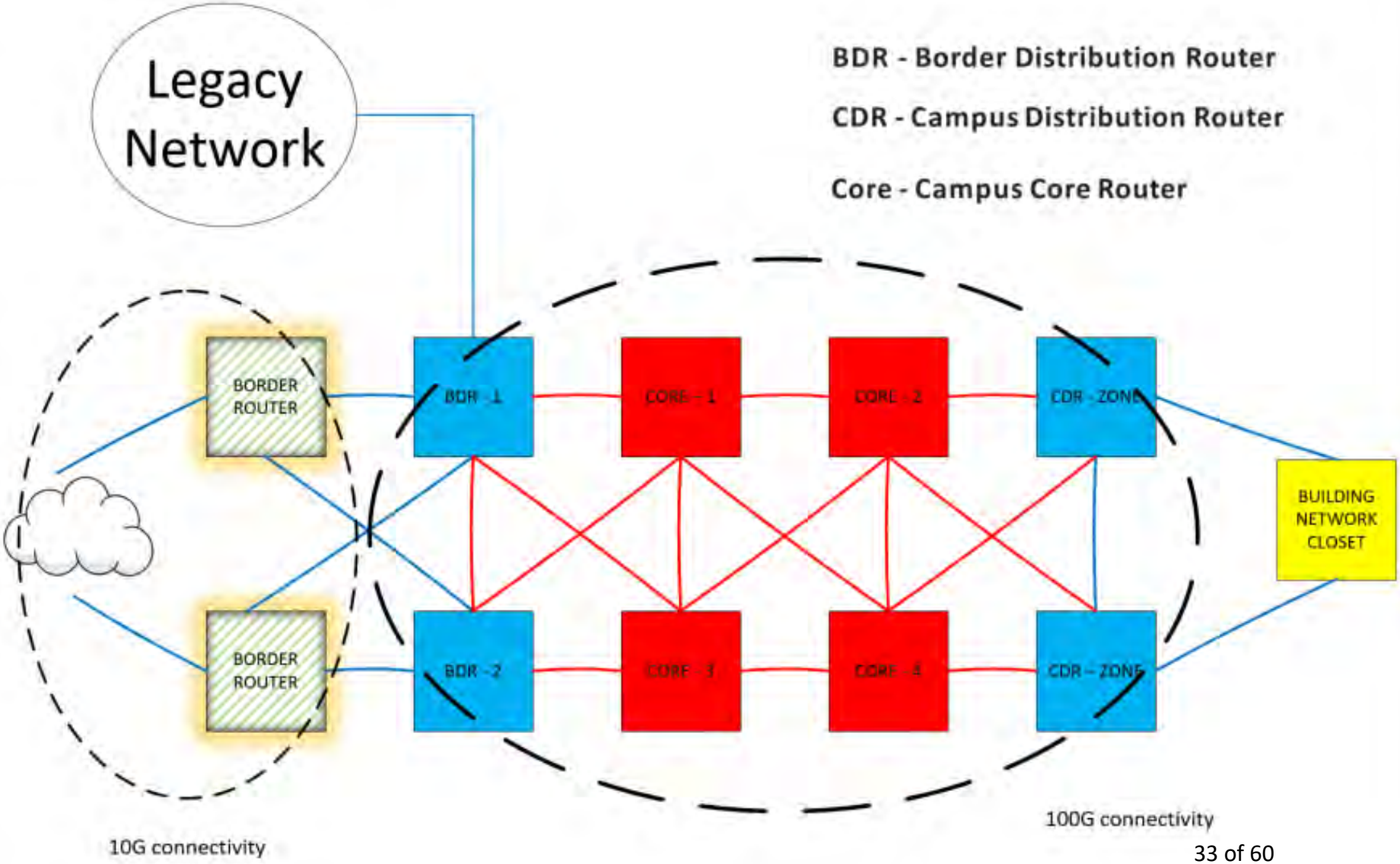
UO Campus Network upgrade



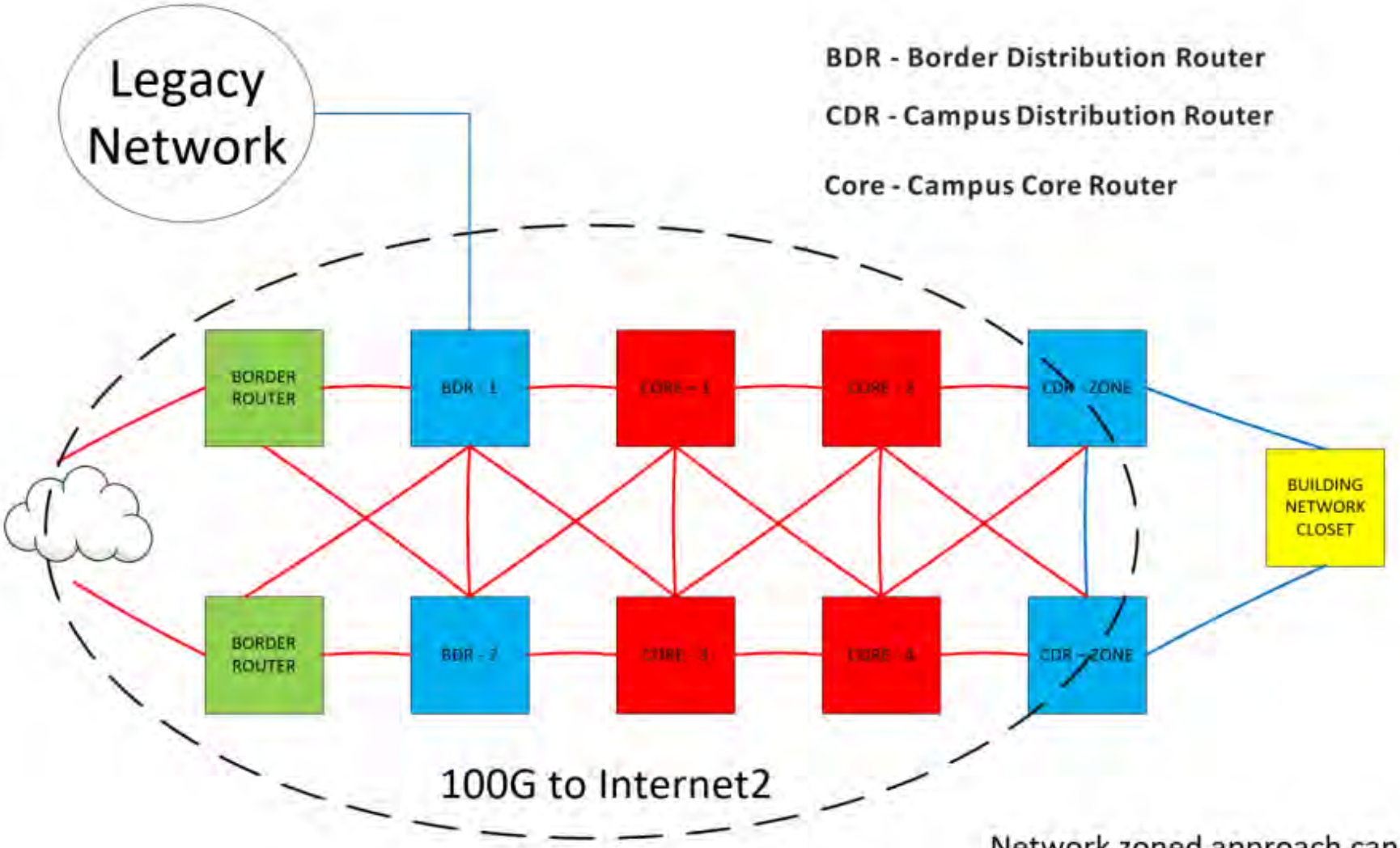
UO Campus Network – before May 2017



UO Campus Network – spring 2017

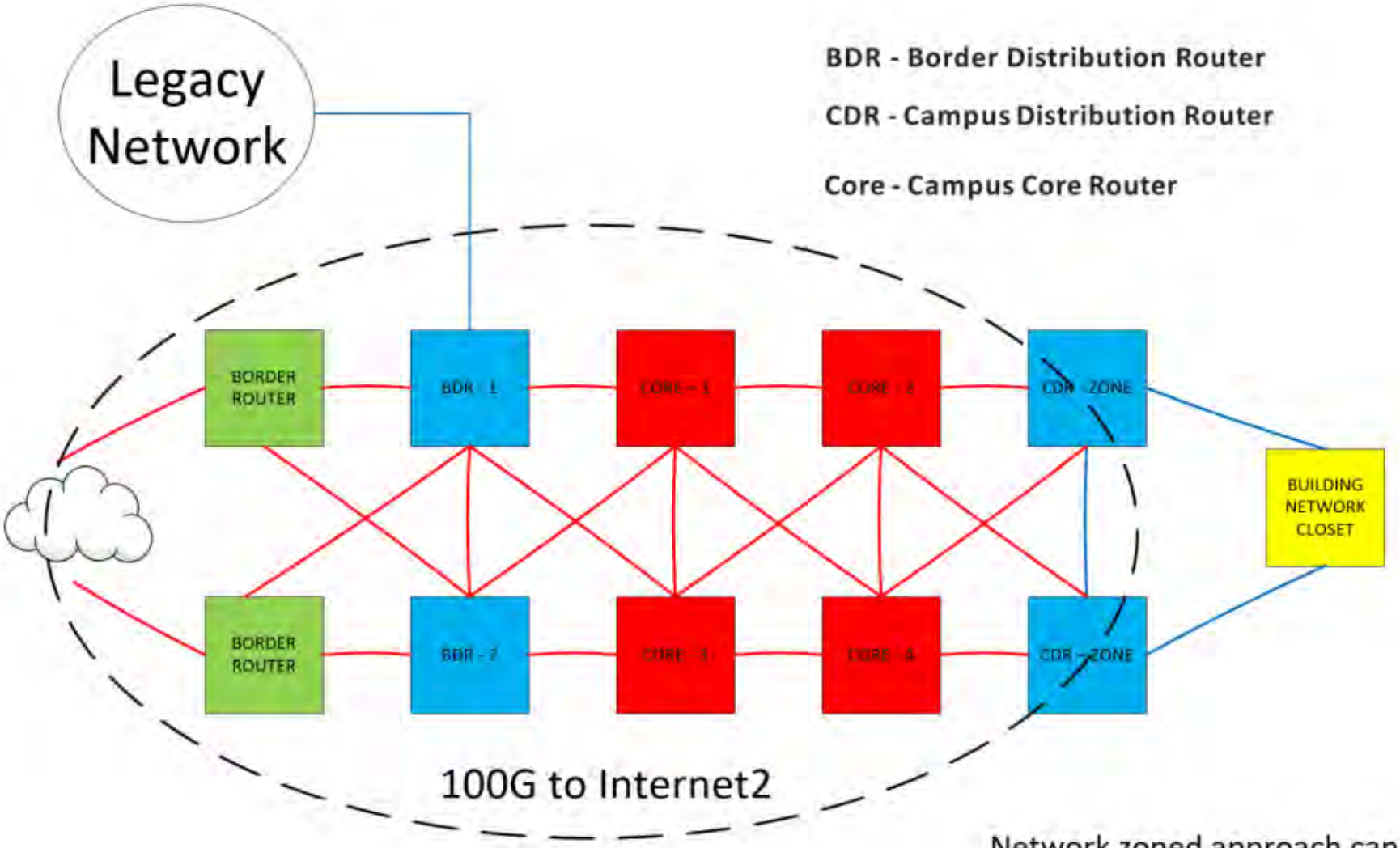


UO Campus Network - May 2018



Network zoned approach can tailor capacity from 1G to 40G at lab/room level within buildings

UO Campus Network – AY19 Plans



Continue migration to retire legacy network (estimated completion Jan 2020.

Network zoned approach can tailor capacity from 1G to 40G at lab/room level within buildings

Oregon FIBER Partnership

Maximizing the buying power of state government and higher education to increase speed, bandwidth, and connectivity

OregonFIBER PARTNERSHIP

Oregon's research universities

- University of Oregon
- Oregon Health & Science University
- Oregon State University
- Portland State University

State government

- Office of the State CIO
- Oregon Department of Transportation

Strong statewide support to date

- Governor's Office
- Oregon Department of Education
- Association of Oregon Counties
- League of Oregon Cities
- OCHIN

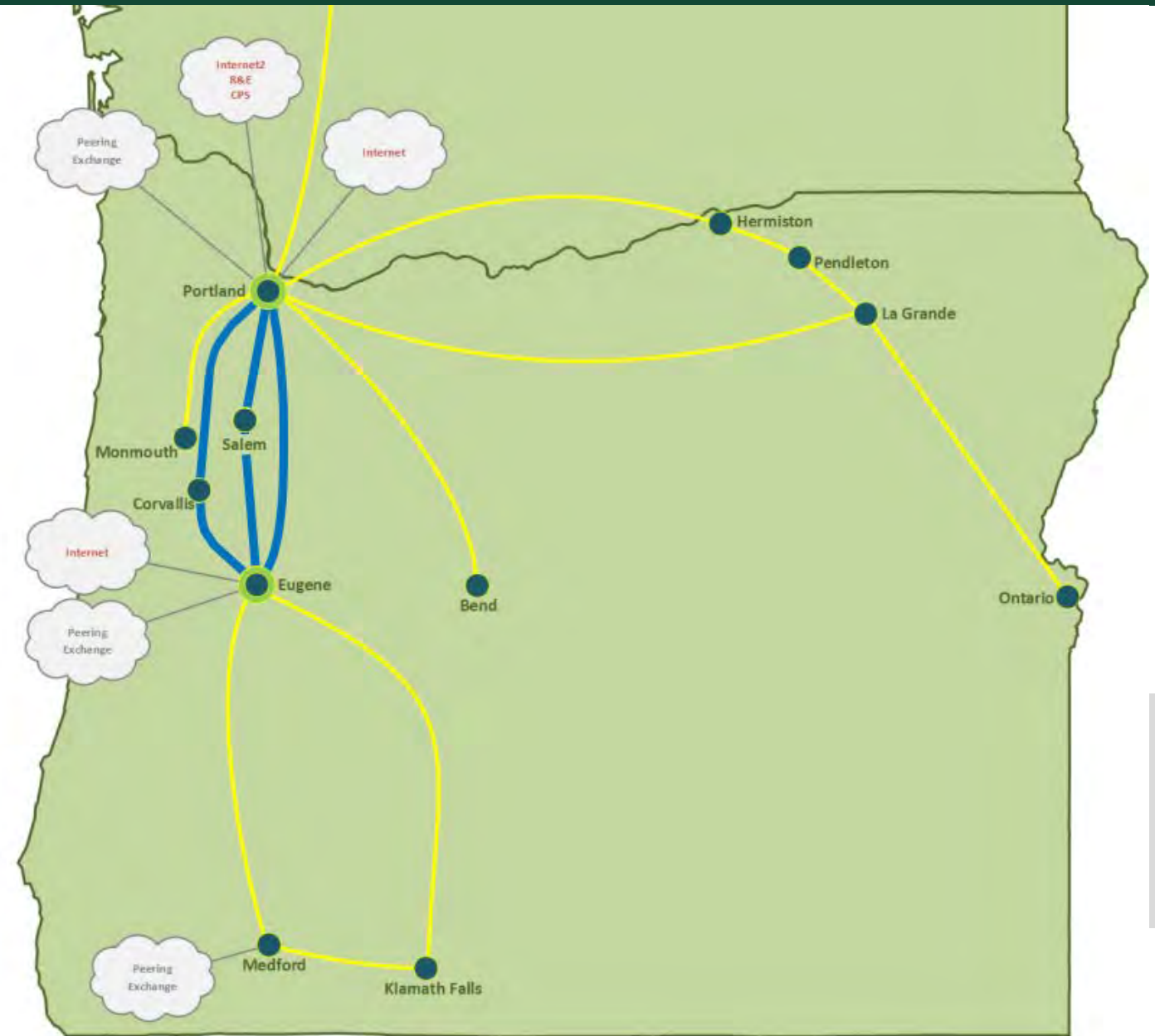
Oregon FIBER Partnership

- Statewide fiber footprint acquired
- Interim operating agreement executed
- Executive Director appointed

HB 4023 Enacted

- Enables OSCIO to serve unserved/underserved K-12, local governments, and tribes
- Established Connecting Oregon School Fund for E-rate matching
- Identifies local broadband champions

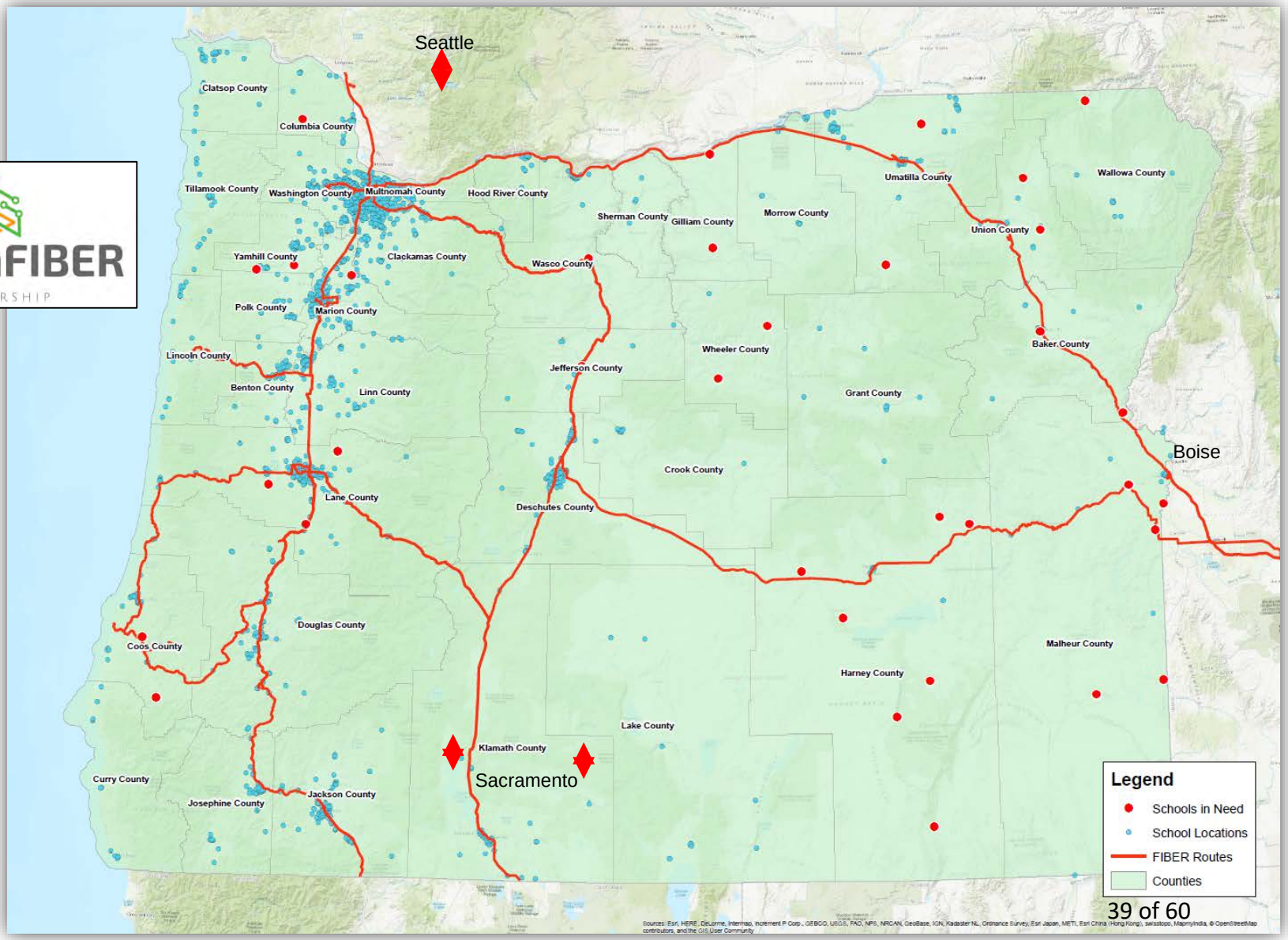
Current Network for Education & Research in Oregon (NERO)



NERO owned circuits at 10G

Leased at 1G or below

Oregon Fiber Partnership: fiber routes obtained



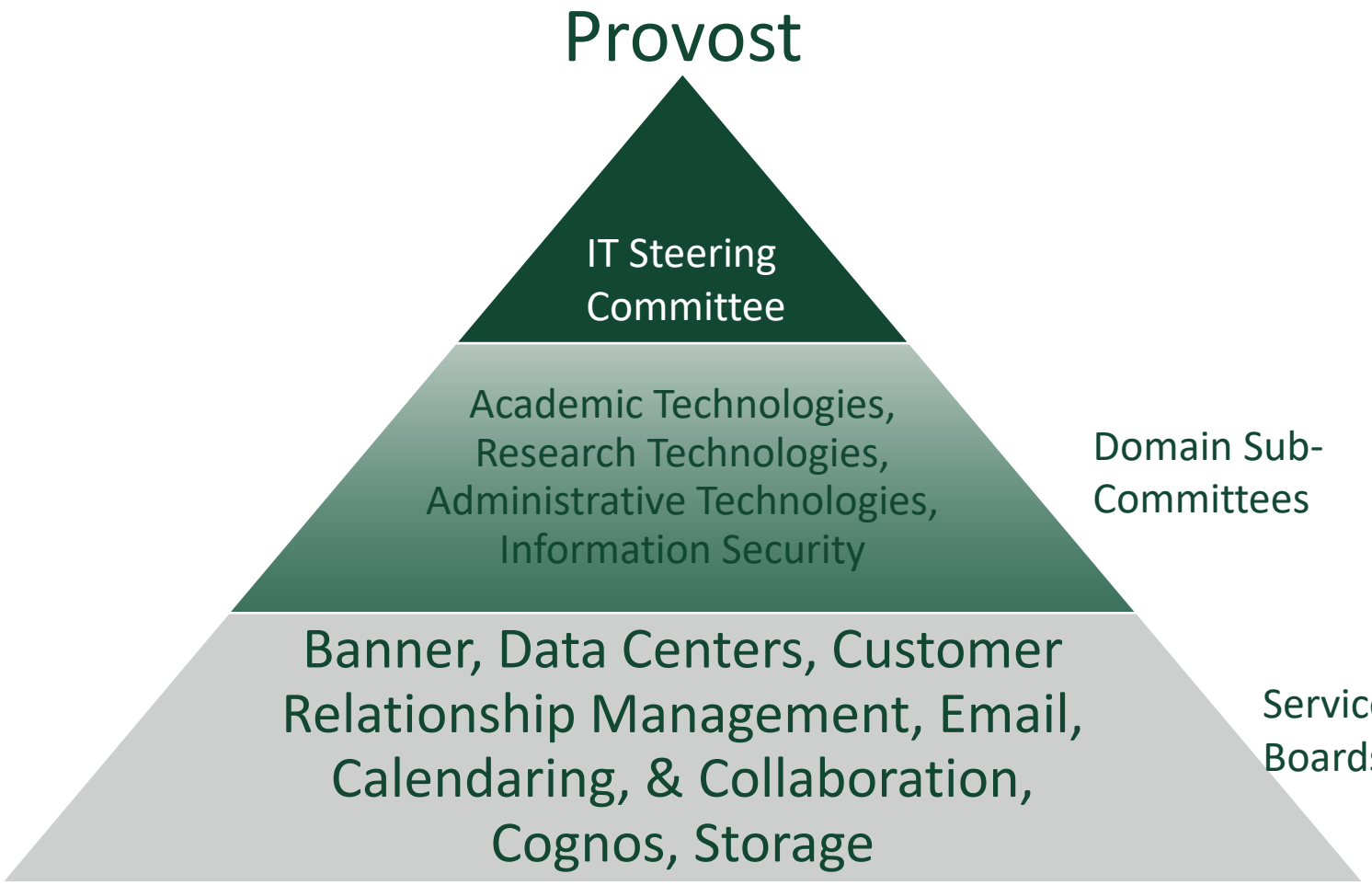
Oregon Fiber Partnership – AY19

- Completion of initial round of fiber acquisitions
- Broadband Services Advisory Committee
  - HB4023 rule making
- Project planning
  - Governance model finalization
  - Business plan/service model
    - Marketing/communications
  - Technical and operations plan
    - Optronics selection
  - Project delivery plan
- In-state and external engagement

Governance

Governance Progress

Approved Jan 2018



Launched spring term 2018

Advisory Groups	
Banner	Email, Calendaring, Collaboration
Data Centers	IDR (Cognos)
CRM	Storage Services

Advisory scope:

- to CIO and/or domain sub-committees on upgrades or funding requests for additional functionality or service offerings
- to service owner on prioritization and approval of modifications/work to be done within existing staff allocated to service

Membership:

- Chair: service owner
- User representation across campus as appropriate by service (including students)
- IT service delivery representation (leadership and technical staff)

Frequency:

- Monthly for most services

Launching summer 2018

Domain Groups
Academic Technologies
Research Technologies
Administrative Technologies
Information Security

Advisory scope:

- to CIO and/or ITSC for requests for new funding, and new service additions
- to CIO/service owner on use of pre-existing funding sources already allocated for service improvements up to $100K

Membership:

- Chair: CIO, CISO, Dean of Libraries as appropriate
- Faculty, Dean, VP representation

Frequency:

- Quarterly

IT Steering Committee (ITSC)

Recharged ITSC

- Revisited membership relative to new groups formed
- Focus on:
  - Prioritization of major initiatives
  - Policy changes
  - Strategic funding recommendations
  - Annual allocation of student tech fee
- Reduce frequency to quarterly
  - Align with annual funding cycles

Foundational Maturity

Transform IT

Foundational IT Maturity Improvements

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

Foundational IT Maturity Improvements

Transform IT: related projects

Spring 2018

Initiated campus move from 60+ distributed email platforms to Exchange Online

Benefits:

- Alumni email for life; Fall 2017 graduates and beyond will retain email address and connection to UO
- Reduced cost, duplication of services
- Reduction of cybersecurity risks
- Elimination of manual provisioning of email accounts

Timeline:

- 33% of faculty and staff not already on Exchange migrated by June 2019
- Auto-provisioning in place by June 2019
- Fall 2017 graduates and beyond retain uoregon.edu email address via forwarding

Technology Risks

Cybersecurity, Compliance, and Resiliency

Cybersecurity/Compliance Risk Mitigation – since Dec 2017

Leo Howell, Chief Information Security Officer, on campus Dec 2017

- Cybersecurity strategic plan development
  - Vision, mission, strategic objectives, goals, and tactics for the next 3 to 5 years
  - A maturity assessment of our program and capabilities and resources needed for improvement
  - Plan developed with input from key business and IT stakeholders, and is being socialized across campus
- Compliance initiatives under way to address
  - Federal Acquisition Regulations (FARs), which require security of federal research data and intellectual property
  - Gramm-Leach-Bliley Act (GLBA), which requires stringent security of financial aid data
  - The EU General Data Protection Regulation (GDPR), which requires stringent security and privacy protection of persons domiciled in the EU
- Information Security and Privacy Governance subcommittee (ISP GC)
  - A domain of the ITSC; a cross-functional team of research, academic and administrative leaders
  - Responsible for providing oversight for university security and privacy programs

Cybersecurity/Compliance Risk Mitigation – AY2019

- Continue to socialize the plan, and secure funding to support the cybersecurity program an appropriate level
- Implement high impact components of the plan and continue to improve compliance including
  - Awareness and training
  - 2-step login or two-factor authentication
  - Secure research services
- Develop partnerships across Oregon (State and higher education) to address high volume of attacks

Resiliency Risk Mitigation – since May 2017

- Effective governance process in place to allocate technology fee for needed infrastructure replacement
- Partitioned end of life equipment to low-risk areas of network
- Robust, resilient core network deployed, legacy network connected to mitigate risk while migration off legacy network is completed
- 100G connectivity established off campus to support competitive research peering and attract world class research faculty

Resiliency Risk Mitigation – AY19 and beyond

Critical Hiring:

- Chief Technology Officer

Initiatives:

- Lead development of IT Strategic Plan to support *Excellence*
- Development of UO technical and architectural strategy
- Implement appropriate approach for disaster recovery, cloud, research support, long-term funding models for infrastructure replacement

Questions?

IT: The New Strategic Imperative

BY: JOHN O'BRIEN

TRUSTEESHIP MAGAZINE | MARCH/APRIL 2018

TAKEAWAYS

Many boards and administrations may be missing opportunities to engage in meaningful conversations about strategic technology, which is not only a key differentiator but also a necessity for meeting an institution's strategic goals and mission.

Some of the greatest institutional challenges that vex presidents and boards—such as the student success crisis—find their most promising remedies in technology innovations and emerging software systems.

Student advising systems, graduation planning tools, and a host of other systems powered by predictive analytics will play a key role in helping institutions realize critical strategic goals.

I registered for college classes so long ago that the most advanced technology I experienced amounted to state-of-the-art clipboards. Today, I occasionally look around in awe when I consider how nearly everything about the student experience at our colleges and universities has changed. For today's students, technology is everywhere, involved in everything we do—and yet we are still in the early years of an inexorable digital transformation. Just as home appliances that communicate with one another on our behalf are reshaping our domestic lives, so too are emerging technologies such as predictive analytics, artificial intelligence, and the internet of things transforming the student experience.

This remarkable moment—when technology is strangely both emerging and ever-present—offers the perfect time for governing boards to reflect on the ways they are engaging in strategic conversations about technology. At EDUCAUSE, we believe that many boards and administrations may be missing opportunities to engage in more meaningful and frequent conversations about strategic technology, which is not only a key differentiator but also a necessity for meeting an institution's strategic goals and mission.

Over the past decade or so, there is convincing reason to wonder how and how much boards should engage on this timely topic. For example, Richard Nolan and F. Nolan McFarlan, in the October 2005 issue of *Harvard Business Review*, acknowledged the growth in IT and concluded that most boards are "in the dark" about IT investments and strategy, noting that, while "dangerous," it "may seem excusable" given the lack of IT governance standards in place at the time. Six years later, AGB's November/ December 2011 *Trusteeship* article "What's the Next Big Thing for Boards?" included a strong call to action relating to technology, concluding that "boards are often not sufficiently tuned in to the 'technology tsunami' that is rapidly threatening to engulf higher education … and we are not ready."

The most recent AGB survey data from 2013 find that, although 71 percent of board members believe online education will be "important" or "essential" at their institutions, only 19 percent feel they are well-informed and demonstrate "appropriate strategic engagement" when it comes to educational technology. Twenty-eight percent "don't know" or characterize their engagement as poor. Our EDUCAUSE data also find evidence of a strategic opportunity that may be missed. For example, even though information security has been at the very top of the EDUCAUSE Top 10 IT Issues for the past three years in a row, 8 in 10 campus strategic plans include no mention of IT risk.

Any disconnect is concerning since information security is such an institution-wide issue. This is true both in the way a security lapse can result in broad financial and reputational damage and in the degree to which cross-divisional collaboration is required to address information security risks. It is no surprise that when we consider where responsibility for information security practices lies, central IT comprises the largest group by far, but in literally every information security area, from network security to data privacy, responsibility is increasingly shared (and in the case of data privacy shared equally). Given that inviting catastrophe takes no more than a single lapse in judgment from only one person, institution-wide collaboration and shared urgency around information security is vital, requiring training, awareness, and action that extend across multiple stakeholders and all campus divisions.

The strategic scope of information technology is not expressed solely through the risks involved, but also through the important strategic contribution IT can and will increasingly make. In fact, some of the greatest institutional challenges that vex presidents and boards—such as the student success crisis (see related article on page 26) and the opportunity gaps that afflict our most vulnerable and underrepresented students— find their most promising remedies in technology innovations and emerging software systems. Student advising systems, graduation planning tools, and a host of other systems powered by predictive analytics will play a key role in helping institutions realize critical strategic goals.

If the governing board at your college or university has not yet engaged with technology as a strategic asset, no one should be blamed. After all, it wasn't terribly long ago when IT was primary understood to be a utility—a remarkable, promising, and often inscrutable utility, but a utility nonetheless. And there is a long tradition of categorizing IT with other utilities, as something that magically works when you turn a tap handle or plug in an appliance. One CIO recently talked to me about this legacy perspective in which IT was expected to be "silently awesome," a utility you didn't really know was there until it broke. Needless to say, this view of IT is about as far from strategic as you can get.

In 2018, it's hard to imagine anyone saying that IT is a utility that can be safely ignored until it breaks. However, if you total the number of board discussions about your campus finances, enrollment, or facilities, how would the number of technology discussions compare? And when technology is discussed, is it assumed that IT is a strategic asset? If the topics that bring technology to the board are responses to specific incidents or *pro forma* budget reviews, the answer is likely no. If proactive conversations about technology strategy, including the impact and potential impact on teaching and learning, are not recurring features on board

agendas, the approach can't be truly strategic, however well-intentioned everyone involved may be.

We should also recognize that at times, some legacy thinking may still exist within the IT department itself. "Many IT leaders are too focused on technology and not enough on the core business of the college or university they serve," said Michael Kubit, vice president for information technology and CIO of Penn State University. "As IT leaders, we need to help executive leadership and governing boards better understand the strategic value of IT as it relates to our institutions. IT organizations should be strategically pivoting from a culture focused on providing services to one of enabling and empowering the use of technology. If IT is perceived as a utility, we have no one to blame but ourselves."

When you are running a utility, protecting the operation and saying "no" may make sense, but as Joshua Singletary wrote in the February 2018*EDUCAUSE Review*, "To be successful in the changing landscape of technologies and user needs, IT will need to become a partner rather than a gatekeeper."

However, it's also possible that even as campus IT functions as a strategic partner, its effectiveness will be stalled if the senior IT leader is not part of the strategic decision-making fabric of his or her institution. How can this be accomplished? How can a governing board best ensure that it is appropriately engaged with technology in a way that limits exposure to risk and unleashes technology innovation? Recognizing that every board and campus culture is unique and that no single solution is perfect for all college and university boards, here are a few suggestions to consider.

ASSESS YOUR CURRENT BOARD ENGAGEMENT AND STRUCTURE

Review how your governing board has taken up technology topics over the past few years. Is a technology committee or subcommittee involved, or are technology discussions ad hoc or subsumed in the context of other areas such as finance or facilities? Establish a structure that provides sufficient discussion and deliberation of the strategic implications of technology, aligned with institutional goals and strategies. If your board is among the 80 percent that are not fully engaged, it's important to explore whether the current structure enables and encourages consideration of a different approach.

In a 2015 *Trusteeship* article, Angel Mendez, a member of the Lafayette College Board of Trustees and the AGB Board of Directors, suggested a number of diagnostic questions for boards, including:

- Does the board regularly evaluate trends in higher education technologies as part of institutional strategy?
- Are IT systems secure and are there up-to-date policies and practices in place to protect the privacy of data?
- Does the institution have a master plan in place for information technology that is well-aligned with the strategic plan for the institution?
- Is there a mature governance model in place, executed at the cabinet level, that regularly reviews requests for spending on IT projects and sets appropriate priorities among them in the context of all other requests for capital and operating funds?
- Are the board committees aware of the return on investment in technology?
- Can the board see clearly how the institution weighs investments in technology within the context of its entire budget?

Mendez writes that the decision to establish a short-term or ongoing technology committee hinges on whether the board has considered these (and other similar) questions and can answer "yes" to most of them.

IS TECHNOLOGY AT THE TABLE AT YOUR COLLEGE OR UNIVERSITY?

While boards explore their level of engagement with technology issues and opportunities, it also makes sense to consider the strategic placement of IT within the campus. AGB's 2017 "Board of Directors' Statement on Innovation in Higher Education" acknowledges that "the technology revolution has only begun," innovation is crucial, and "boards should ensure that campus technology professionals are thoroughly involved in those projects that depend on technology for their success." In addition, the statement argues that "presidents must also consider the strategic placement of technology within the organization," concluding that "it will prove difficult for technology to serve as a strategic asset for innovation if the CIO is not at the table when key decisions are made at the cabinet level."

There is no question that having the campus CIO reporting to the president or chancellor is a surefire way to ensure that IT is "at the table," but reporting lines may not always be the instrument that ensures an appropriate degree of strategic influence. The essential need is for the

CIO to serve on the president's cabinet. EDUCAUSE research shows that when CIOs serve on the cabinet, they are far more likely to discuss the broader implications of IT with executives and shape institutional strategic directions, including those academic directions for which technology offers such promise.

EDUCAUSE Core Data Research maps out the opportunity, finding that less than a third of senior IT leaders currently report to the president/chancellor, and just over half (55 percent) sit on the cabinet, numbers that have not changed considerably over the past decade. In another EDUCAUSE survey, only 44 percent of CIOs say they experience "alignment among institutional leadership," evidence that inclusion in the cabinet is likely the best way to strengthen strategic considerations of technology. The alternative is risky, as retired former EDUCAUSE presidential fellow and CIO Brian Voss recalls. At one campus, he was told that even though he wasn't serving on the cabinet, he should rest assured that "if there are any IT issues, we'll call you in." Instead, he was left wondering how, without IT at the table, anyone would be able to know when or whether to make that call—or whether the call would come too late.

Invariably, information security risk is a powerful exclamation point when it comes to talking about IT's strategic role because the stakes are simply so high. In a February 2018 report issued by EDUCAUSE and Deloitte's Center for Higher Education Excellence, Phil Ventimiglia, Georgia State University's chief innovation officer, is unmistakably clear: "If you really believe in cybersecurity and the importance of technology to the operation and future of the campus, then the CIO or whatever role is leading technology for the institution should be at the cabinet level." This strategic placement within the campus cabinet is a two-way street, as Neil Kerwin, American University president emeritus, insists. "With a seat on the cabinet," he said, "the vice president of information technology educates colleagues on the senior management team and is educated by them. That works its way ultimately up to the board of trustees."

INCLUDE INFORMATION SECURITY IN RISK MANAGEMENT REVIEW

In 2014, AGB published a "wake-up call" report that lamented lack of governing board engagement on enterprise risk management (ERM) and issued a call to action, noting that ERM "offers an approach for assessing threats and seizing opportunities" that governing boards should adopt. At that time, fewer than four in ten boards actively used ERM processes, and among those that didn't, half had no plans to do so. ERM demands that consideration of risk not be done on a reactive basis, and it's easy to see how an established ERM approach by a campus governing board encourages the kind of proactive strategic approach to IT advocated here.

While board discussion about the risk of an information security breach may not be the most calming conversation for a CIO or chief information security officer (CISO), discussions about risk can easily give way to conversations about the strategic lynchpin that technology has and will increasingly become. A typical ERM chart, like the one from the University of Wisconsin's 2010 Enterprise Risk Management Handbook, includes IT risks such as an "IT system failure." On the one hand, this reinforces the potential danger of an IT system crisis; on the other hand, it also reinforces the strategic value and institution-wide criticality of IT. Handled with care by a forwardfacing governing board, a conversation that starts with the risk of an IT

failure will evolve into a conversation about the potential, promise, and value of technology across the institution.

A CAUTIONARY NOTE: TAKE THE HIGH ROAD

When boards turn their attention to technology and deepen engagement in technology issues and opportunities, it's important to settle into the right altitude. IT matters can sometimes pull even the most disciplined board down into the weeds of operations, a situation that benefits neither governance nor management. The strategic engagement I am recommending should never devolve into depriving campus leadership of the right and responsibility to manage and lead appropriately. Ultimately, board micromanagement and operational involvement risk delays, declining morale, and diminished organizational effectiveness, and distract the board from the effective execution of its fiduciary duties. Balanced and thoughtful engagement with an IT leader responsible for managing strategic assets brings out the best in everyone and builds a triangle of trust among the governing board, the president, and IT leaders.

A few years ago, my son was trying to call a friend, but the cellphone froze up. He was doing that thing where we push buttons harder in case that will help the software work better. Eventually, he let out an exasperated sigh and said, "I can't dial any numbers on this stupid phone!" Then he froze and looked at me, intrigued. "Wait a minute," he said, lifting up the offending device. "Why do we say dial a phone?" The reason is that technology moves faster than language—faster, in fact, than just about anything these days. As challenging as the race may be, college and university boards and leaders must commit themselves to keeping up—not only with the technologies, but also with the people, processes, polices, and governance. The sooner we give both the challenges and the opportunities our full strategic attention, the better.