Information Technology Ecosystem/Security, including Risk Management Report

BACKGROUND

The Executive, Audit and Governance Committee annually reviews the top risks that may impact Oregon State University's ability to meet its mission and objectives with university leadership. Each of the top risks identified are assigned to the various board committees based on alignment with each committee's charter and workload. Through this process, the university identified OSU's *information technology ecosystem and security* as a top risk for the university. Within this risk area, three objectives have been identified to be tracked. The Executive, Audit and Governance Committee provides oversight of the university's action plan for mitigating this risk.

VISION

The Division of University Information and Technology (UIT) is working to protect the OSU community and digital assets by implementing resilient, compliant, and functional access to systems, services and data based on a zero-trust architecture. When the four pillars of our zero-trust architecture – identity, endpoint, application, and data – are in place, UIT will be positioned to protect OSU data assets and community members, granting every member of the OSU community a single, authoritative identity, supporting multiple roles, providing secure access to the right data, applications, and systems, from any device, at any time. OSU devices will be managed to ensure access to data, applications and systems are controlled in line with institutional risk and governance, freeing OSU data as an available strategic asset. Cloud-based by design and architected in line with the university's risk appetite and business requirements, the resulting IT ecosystem will enable OSU to manage risk and assure service in contested cyber space. In collaboration with the Chief Data Officer (CDO) and the data team, the zero-trust environment underlying this IT ecosystem will protect and empower OSU community members, supporting their needs and the mission of the university. It will meet the regulatory and competitive compliance requirements applied to the university.

ADDRESSING THE RISKS: IT AND DATA ECOSYSTEM

The OSU data environment is complex. We have an abundance of data elements we collect, nurture, disseminate and archive, yet we lack efficient access to the data needed to easily develop insights and make decisions. Historically, we have devised alternative solutions, with varying results, often duplicating efforts and data. Many of these solutions were unknown and unmonitored by our formal security efforts, resulting in the risk of individuals having access to data they do not have security clearance for and/or sensitive data being exposed. For example, Banner, OSU's Enterprise Resource Planning system, requires integration with 25 systems to support 2,000 administrative users providing critical HR, finance and procurement activities and supports 35,000 student users. Fifty databases support operational and reporting environments. CORE, our primary reporting, and data environment for OSU central operations, includes 28 reporting domains and 1,500 standard reports, averages 3,000 users annually, and provided 958,000 report views to users in 2022. One of the key strategies in the IT Strategic Plan is focused on securing and freeing OSU's data to enable and support the university's

missions. With the addition of our CDO, we have advanced our efforts to build a robust and unified Enterprise Data Ecosystem.

Progress Report
Securing the data environment is foundational to enabling the use of data as a strategic asset in line with OSU's values and expectations. To that end, we are implementing a Data Hub and an Integration Hub which will serve as the core of OSU's redesigned data ecosystem.

Major progress has been made to lay the groundwork and design a modern, cloud-based platform to ingest, store, model, and provide access to data.

- Completed initial design and architecture for an underlying Data Hub and Integration Hub (DIHUB) platform, enabling new capabilities in our data environment to resolve long standing pain points and creating the foundation for the Administrative Modernization Program (AMP) in a modern and scalable approach to ingesting, managing, governing, securing, and providing data to an empowered community of data users.

- In Spring, we will test secure access to standardized university data assets via a cloud application. This will change and modernize the way users connect to data and our ability to monitor and understand who is accessing data and how it is being used is being used.

- The DIHUB and Identity and Governance Administration project teams have collaborated to define work around role definition and access planning.

- Planning has begun to enhance the monitoring and data security capabilities in our new data ecosystem.

Objective 1 in the Attachment 1 table lists the associated actions and their status.

STRENGTHENING THE INFORMATION SECURITY PROGRAM

The Office of Information Security is leading the Identity and Access Management and the Endpoint Management Teams. The work of these teams and an addition of a Deputy Chief Information Security Officer in fall 2021 have measurably increased the capacity of the Information Security Program.

The institution's information security program continues to mature, using the NIST Cybersecurity Framework as a benchmark. The September 2022, the NIST CSF assessment showed an 8.6% improvement in maturity compared to the November 2021 assessment. The increase in maturity reflects improvements in all areas of the NIST CSF: Identify, Protect, Detect, Respond and Recover.

Progress Report
Major Program achievements over the last year are listed below:

- A work group was formed to review OSU's compliance with the Gramm-Leach-Bliley Act (GLBA), and a process was developed to ensure risks associated with holding sensitive customer data are mitigated. This group is also reviewing the new GLBA Safeguard Rule which takes effect in June 2023.

- The Office of Information Security has been partnering with the Research Office to support high-compliance research requirements; seeking ways to be more competitive for grants; and to ensure OSU is compliant with the requirements of NSPM-33, particularly for cybersecurity requirements of the research security program.

- The university undertook a cybersecurity tabletop exercise for the IT Community and the Controller's Unit, led by the Cybersecurity and Infrastructure Security Agency (CISA), testing OSU's ability to respond to likely cyber threats.

- We are continuing to invest in OSU's Cybersecurity capability, resulting in two members of the Office of Information Security gaining cybersecurity professional certifications, qualifying a member of the security operations center in digital forensics, and continual improvement in detection and response tools.

- We established a Vulnerability Management Committee to encourage more rapid mitigation of discovered defects in system security.

- We published two information security rules (Digital Identity and Access Management; Third-Party Risk Management) and updated the Acceptable Use of Computing Resources Policy.

- Three additional full-time positions within the Office of Information Security have been authorized, with a goal of hiring this fiscal year, expanding capacity and student engagement and learning with the hiring of a total of 15 students.

- OSU has moved quickly to adopt a set of "Common Tools" to manage endpoints. The legacy Microsoft management system was reduced from four instances to one, and the system managing Apple products was simplified and moved to the cloud for increased resilience. In Spring, management of Microsoft endpoints will start the move to the cloud as well.

- Dashboards and reports have been produced to track risks over time and enable the IT community easier access to actionable tasks. This has resulted in a measurable reduction of risk across the enterprise and supports the vulnerability management teams.

- UIT, the Division of Extension and Engagement, College of Agricultural Science, and Link Oregon created a new statewide network to bring the Extension County Offices and Agricultural Experiment Stations inside the OSU security boundary, providing significantly improved IT oversight and protections. The first site was migrated in November of 2022, the Eastern Oregon Agricultural Experiment Station in Burns, Oregon.

Other elements of the IT Ecosystem also received attention over the last year to address risk and improve support and service to the OSU Community:

- We established a plan to migrate students to Microsoft Exchange online to improve integration with faculty and provide better cybersecurity protection; new students receive Microsoft services now and existing students will be migrated this summer.

- In partnership with the Chief Human Resources Officer, the Human Resources Service Delivery project was deployed in February 2023, replacing an antiquated system, improving customer experience and the security of information.
- "Get Stuff Done" (GSD) teams engaging OSU IT staff across campus have been launched to address high risk IT priorities (e.g., standard configurations of systems, improved communications, change management, standardized service delivery) and reallocate IT resources to strategic efforts. Intermediate goals were achieved in September, and GSD improvement goals are due by the end of June.
- We established the Enterprise Information Investment Committee as the top-level IT governance group to ensure IT investments and risks are managed in line with OSU's values and missions.

Objective 2 it the Attachment 1 table lists the associated actions and their status.

IDENTITY AND SMART ACCESS

The ability to lead vibrant, digitally empowered lives at OSU in support of instructional, research, extension, and service missions requires OSU community members to have secure access to the right information whenever they need it, whatever role they hold, and with any device they use.

Progress Report
Major Program achievements over the last year are listed below:

- In September 2023, a vendor and an integration partner were selected to implement OSU's Identity and Governance Administration (IGA) tool. A two-year plan to transition OSU to a single identity and access control system and retire legacy systems was developed.
- By the end of the current fiscal year, the university's current "ONID" accounts will be transitioned to the new IGA. This effort will involve over 100,000 accounts and improve our ability to support and manage those accounts.
- Also by the end of this fiscal year, an initial set of Zero Trust Conditional Access policies will be implemented to demonstrate that the Zero Trust strategy is sound.
- Planning for IGA support of other high priority projects, such as the Student CRM effort, is underway.

Early in the next fiscal year, our efforts will move to transitioning other account types to the IGA and creating "roles", or specific set of data and systems access requirements associated with certain tasks (e.g., Advisor) to improve access to data for those that need it and prevent access for those that do not have the need.

Objective 3 in the table in Attachment 1 lists the associated actions and their status.

EMERGING RISK AREAS

Over the past year, new areas of technological, compliance and cyber risk have increased and therefore incorporated into the IT Roadmap.

Technology and Compliance

- OSU is in the preliminary stages of modernizing its core administrative systems to gain the agility needed for new university business models, program designs, and to increase efficiency. This effort is called the Administrative Modernization Program (AMP). An unwillingness to move to new systems and processes is a potential threat we are addressing with the assistance of our consultation partners and planned engagements such as the AMP Preparedness Podcast series and the AMP Leadership Bootcamp.

- Technology innovations and new capabilities, such as generative AI (e.g., ChatGPT) have the potential to transform the education experience and be disruptive at the same time. OSU needs to be aware of new technologies and be positioned to maximize their benefits while managing disruption and mitigating risk. The OSU IT Community collaborated with the Senior Vice Provost for Academic Affairs on a workgroup that reviewed the challenges and opportunities of ChatGPT and other artificial intelligence tools for teaching and learning at OSU. The next steps are to support the success of Academic Affairs' recommended guidelines and practices, standardize our communications and socialize throughout the OSU community.

- Federal and state Governments continue to place restrictions on technology that raises national security concerns. In 2019, OSU was required to validate that the institution did not use any IT equipment from certain embargoed Chinese companies. More recently, the use of TikTok by some federal and state agencies has been banned. In some states, such as Texas, the state ban extends to higher education institutions. Oregon does have a legislative proposal to ban services and applications from ByteDance, the parent company of TikTok. The federal ban could extend to entities that accept federal funding. We are tracking this closely to mitigate any risks to OSU.

Cybersecurity

In November 2022, Microsoft released their annual Digital Defense Report detailing increasing cyber aggression targeting higher education. The report highlighted the "ferocity, scope, and scale" of ransomware and other cyber-attacks. Increasing digital threats, combined with changes in our cybersecurity insurance coverage, demonstrate the need for hyper-vigilance to defend our community and digital ecosystem. Priorities include continued deployment of security tools, increasing our capability to detect and respond to suspected ransomware, addressing the security of the Internet of Things, and timely completion of system updates as patches are made available.

NEXT STEPS

At its April 13 meeting, the Executive, Audit and Governance Committee will review the risk management report with staff and may identify additional follow-up actions, as needed.

Oregon State University
Enterprise Risk Management
2022 Priorities
Information Technology Ecosystem/Security

Risk Topic Oversight Summary						
Board Oversight Committee	**Risk Topic**	**University Goal**	**Type(s) of Risks to be Prevented**	**Risk Owner(s)**	**Primary Risk Mitigation Strategy(ies)[1]**	**Risk Mitigation Team**
Executive, Audit and Governance Committee	Information Technology (IT) Ecosystem/Security	Effectively implement the OSU IT Strategic Plan; provide for a data driven enterprise; and safeguard IT resources against loss of research, operational or student data; safeguard network services to prevent disruptions of service, financial loss, or negative perceptions of operational controls and maintain compliance with national security laws	Operational, Compliance, Financial, Reputational	Provost, Vice Provost for Information Technology and Chief Information Officer (CIO)	Accept, Reduce, Share/Insure	Chief Information Security Officer; Executive Director, Technical Solutions Architecture; Executive Director, Business Architecture; Executive Director, Enterprise Architecture; IT Security Advisory Council

[1] Definitions of mitigation strategies:
Avoid: Discontinue the activities that present unacceptable risk
Reduce: Implement controls, practices, programs to lessen the risk
Share/Insure: Transfer the risk through insurance programs or 3rd party
Accept: Proceed with the activity because the benefit outweighs the risk

OBJECTIVE 1: Build a robust and unified university data/information ecosystem that delivers data as a strategic working asset	
Actions to Satisfy Objective	**Status Report**
Enterprise Data Ecosystem a. Data governance Council, Steering Committee and working groups develop and adopt new processes and policies that enable a more trusted, secure, and accessible data environment. b. Engage with industry experts to validate and advance data and integration hub plans. c. Complete Security and Enterprise Architecture reviews for the Data and Integration Hub projects d. Deliver by June 30, 2023, Data and Integration Hub 1.0 deliverables, including working pipeline and delivered data that supports a critical business function adhering to security requirements (pre-AMP) e. Release data products to leadership and their analysts in a secure cloud-based platform, marking a notable change in both the type of data that are made available and enabling increased security measures to both protect and free our data.	**Completed and Planned Activities** a. Data Governance: • Data Governance processes established to define roles and provide expanded access to data. • Improved Data Governance process and partnership to manage and validate data products released in the enterprise data ecosystem, increasing the standardization, validity, and reliability of our most critical data. • Deployed secure virtual data warehouse environment leveraging HelioCampus platform starting with enrollment and student success data. Broad campus release of validated dashboards and data models scheduled March and April 2023. b. Developed a working plan to test hub capabilities at a small scale. c. Completed Data and Integration Hub 1.0 architecture and selected initial business cases to build an elegant cloud-based process to deliver of data as a strategic working asset d. June 30 Deliverables: • Completed "Where is our Data" maps aligned with initial AMP efforts, providing a guide to for the systems and data flows that will be part of AMP phase I. • Documented critical business processes & critical systems for HR, Finance, and Budget Office in the planning for AMP phase I e. Release data products: • Mapping of current MOUs and most frequently accessed data in CORE reporting environment to identify key data elements to drive plans for delivering operational data for critical processes and system integrations. • Release of IQ Insights Collections and subsequent training to campus leadership and analysts

OBJECTIVE 2: Strengthening OSU's Information Security Program	
Actions to Satisfy Objective	**Status Report**
Information Security Program **Identify** a. Update Information Security Resilience Plan and Roadmap based on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) to guide maturation of program. b. Information Security Advisory Committee (ISAC) governance c. Publish and update information security rules. d. Move to a Common Tool strategy to manage endpoints. e. Establish vulnerability management committee. f. Establish GLBA Workgroup and Sensitive Data Workgroup **Protect** g. Onboarded Identity and Access Management team to the Office of Information Security h. Revitalize awareness and training program. i. Workgroup charged with developing standard configuration baselines for workstations. **Detect** j. Centralize network, application, and endpoint anomaly detection. k. Implement and maintain continuous monitoring. l. Detection processes in place and constantly improved and refined. **Respond** m. Mature the incident management system. n. Implemented automated analysis and mitigation functions.	**Completed and Planned Activities:** **Identify** a. The program is assessed to have increased 16% in maturity over the last year and the updated Resilience Plan and Roadmap are in draft form to be published in the Spring. b. The ISAC is working on Risk Assessment strategies and reviews the Resilience Plan and Roadmap. c. Two information security rules published, and one Policy updated. d. Reduced from 4 to 1 Microsoft endpoint management system and moved Apple management to the cloud. e. Work on internet facing risks on-going; establishment of standard configurations to be published by end of June. f. Prepared for new GLBA Safeguard Rule and developed guidance for managing sensitive data types on campus. **Protect** g. IAM Team successfully integrated. h. Information Security Critical Training updated; new OSU security resources on web site, and tabletop exercises conducted for staff. i. Final recommendations for configuration guidance due by the end of June. **Detect** j. Anomaly detection has been centralized. k. Continuous monitoring and detection processes in place and constantly improved. l. Detection processes in place and are constantly improved. **Respond** m. Incident response documentation published, and incident commander qualification process is in place. n. Microsoft Dedicated Support Engineer has helped move response to matter of minutes.

OBJECTIVE 3: Protect Oregon State University information assets and stakeholder privacy in line with university values	
Actions to Satisfy Objective	**Status Report**
Identity and Smart Access Program a. Identity and Governance Administration b. Azure Active Directory c. Zero Trust Architecture	**Completed and Planned Activities:** a. Vendor and integrator contracted, with initial operational capability by June 2023. b. Effort to build resilience into the OSU IT Ecosystem and simplify IT; work to begin in Spring 2023, focusing on credentials and device management. c. In June 2023, ZTA initial operational capability delivered.

Performance Metrics		
OSU CSF Risk Profile for Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) systems and data		
Goal	**FY2023 Results**	**Comments**
Identify: 3 Protect: 4 Detect: 3 Respond: 3 Recover: 4	Identity: 2.04 (+11.7%) Protect: 1.94 (+9.5%) Detect: 2.32 (+9.2%) Respond: 2.37 (+9.6%) Recover: 2.33 (+10%)	Higher numbers better. OSU CSF Risk profile—Briefed to CEC in September 2019 and March 2021. Reassessed in November 2021 and September 2022. Percentage increase reflects change from November 2021 and September 2022 assessments.
Deliver training and resources to employees		
Goal	**FY2023 Results**	**Comments**
100% participation in employee and student worker training. Awareness and Training is a key element of the Protect functional area.	Delivered 62% of Staff and 50% of students as of 27 Feb 2023.	In January 2023, the Information Security critical training module became an annual requirement. The current level of training completion reflects that all learners were required to retake this training starting in January.