Information Technology Ecosystem/Security, including Risk Management Report

EXECUTIVE SUMMARY

This report addresses three areas within the university's information and technology ecosystem identified as top institutional risks. The Executive, Audit and Governance Committee focuses on the following integrated objectives: modernizing the university data ecosystem, maturing the Information Security Program, and protecting information assets and stakeholder privacy.

Key takeaways:

- OSU is establishing data as a strategic enterprise asset through the Data Modernization Pathway, to deliver a secure, authoritative foundation for decision making, cross domain reporting, and future AI enabled innovation.
- The Information Security Program continues to mature, under National Institute of Standards and Technology Cybersecurity Framework 2.0 with significant gains in the Governance function driven by clarity in enterprise risk appetite, policy development, and increased oversight of compliance requirements.
- The Smart Access Program is strengthening identity, device, application, network, and data controls using zero trust principles. Operational improvements in identity security, monitoring, vulnerability management, and incident response have materially reduced institutional risk as evidenced by a nearly 79% reduction in compromised accounts over the last 4 years.

BACKGROUND

Annually, the Executive, Audit and Governance Committee reviews the top risks that may impact Oregon State University's ability to advance its mission and meet strategic objectives with university leadership. These risks are then assigned to the various board committees based on alignment with each committee's charter and area of responsibility. Through this process, the university identified OSU's information technology ecosystem and security as a top institutional risk, with three objectives established for ongoing monitoring. The Executive Audit and Governance Committee provides oversight of the university's plan for mitigating this risk.

VISION

Oregon State University's strategic plan, *Prosperity Widely Shared*, is a clear and ambitious guide for the institution's growth and positive impact on Oregon and the world. Technology and the flow of digital information are foundational, enabling the initiatives and capabilities that drive the university's strategic goals.

OSU envisions its community members as leading vibrant, digitally empowered lives and exerting a transformative impact at OSU and beyond. To achieve this vision, five strategic areas have been developed:

- The Administrative Modernization Program (AMP) to ignite organizational and digital transformation across the university.

- Data as a Service: Implementation of a sophisticated cloud-based system to deliver data products that carry significant strategic value for the institution and enable AI capabilities.
- Research: Elevating researchers at OSU; supporting the university's land, sea, sun, and space grants; and architecting an easier-to-navigate, university-scale digital research ecosystem.
- Enabling the university mission: Continuing to build an OSU IT ecosystem that elevates teaching and learning, research, and outreach.
- Inclusive economic development: Improving digital equity, reducing barriers for Oregon and Tribal communities, and increasing participation in the digital economy and society.

MISSION

Oregon State University's information and technology enterprise advances the university's academic, research, and outreach mission by serving as a strategic partner in institutional leadership, transformation, and innovation. We enable the university community to achieve its goals through trusted, secure, and modern digital capabilities that support learning, discovery, and operational excellence by:

- Co-leading institutional strategy, transformation, and organizational change by ensuring that technology, data and digital capabilities are fully integrated into OSU's academic, research, and administrative priorities.
- Designing, governing, and evolving an enterprise digital ecosystem of data, platforms, services, and infrastructure that is secure, interoperable, and aligned to OSU's long-term direction.
- Protecting OSU's digital assets and institutional trust through strong cybersecurity, privacy, risk management, and compliance practices.
- Enabling people and organizations to succeed through change by embedding organizational change management, user-centered design, accessibility, and adoption into all technology initiatives.
- Stewarding resources responsibility through transparent investment decisions, lifecycle planning, and sustainable funding models.
- Continuously innovating as a trusted partner by bringing forward emerging technologies, best practices, and professional expertise to advance teaching, research, and administrative operations.

DATA MODERNIZATION PATHWAY: PROGRESS AND ACHIEVEMENTS

Data is a strategic asset. OSU's data enterprise must be agile, competitive, and secure. The Data Modernization Pathway initiative is leveraging its collaboration with Microsoft to stay at the forefront of technological innovation and industry standards, positioning OSU as a leader in data-informed decision-making. All planned activities under this project are complete, and on-going efforts reflect a commitment to sustaining a resilient, secure, and flexible data infrastructure that supports our mission and strategic goals.

Key Achievements**:**

- **OSU Data Platform:** Developed enterprise data pipelines and modeled key data domains to enable valuable data insights and facilitate the evolution of data-informed decision making.

- **Data Governance**: Continued to mature data governance practices by formalizing processes, clarifying roles and responsibilities, and enhancing data literacy across the university. Stewards have established regular cadence.
- **OSU Data Dictionary**: Developing a comprehensive data dictionary, standardized data definitions, including 21 new student-success definitions. This sets the stage for implementation within a centralized tool.
- **Strategic Dashboards**: First-Year Registration and Retention, College Research Award, Student Achievement and Mission Fulfillment
- **Preparation for Workday Operational Reporting**: Preparing functional teams with the knowledge and practice to create operational reports within Workday environment

Next Steps**:**

- **Data Platform Migration:** Establish OSU Data Platform as the authoritative source for institutional cross-domain and legacy reporting, unify data practices that will set the foundation for AI-supported innovation across the university. Develop and socialize data roadmap with functional units.
- **PWS Advisory Group**: Consolidate all student data to significantly enhance analytical and tracking capabilities, enable robust cross-domain reporting, and position data assets to power enterprise-level AI capabilities.
- **Enablement of new integration platform:** OSU will soon enable a new platform for integrations across the enterprise systems. This will go live ahead of AMP and support all Workday integrations moving forward.

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

Progress Report

The Data and Information Technology Action Plan aligns OSU's IT strategy with the overarching goals of Prosperity Widely Shared (PWS). This plan reflects full alignment across UIT, college, research, and administrative IT units with PWS high-level targets. It includes documented and published metrics to track progress and measure success. The accompanying IT roadmap is a dynamic 18-month set of actionable plans where programs, projects, and efforts are described, prioritized, and resourced to achieve these objectives.

Several areas of focus have a significant impact on securing OSU’s data and mitigating other potential areas of risk:

- **The Administration Modernization Program (AMP):** The university is on time and on budget to deliver Workday, a cloud-based software supporting financial management, post-award grant administration, and human resources to modernize administrative processes and replace the university’s core administrative information technology systems. AMP has completed end-to-end and unit testing, establishing the foundation for a comprehensive user experience review launched in early 2026. The program continues to expand training and skill development opportunities to prepare OSU employees for new ways of working. This includes a cohort of Workday Foundation Liaisons to provide departmental support and direct assistance to university personnel.

- **Artificial Intelligence (AI):** As part of our ongoing commitment to innovation and operational efficiency, we are actively evaluating and integrating new AI-based features within our existing platforms. Foundational tools (e.g. Copilot, Zoom AI, and Workday)

provide secure, equitable access to AI in approved and governed enterprise systems. Through rigorous change-management practices and strong oversight of the enablement process, we are ensuring a smooth and secure transition across our environment.

- **Research:** OSU launched the Research Computing Office to implement a scalable, centrally coordinated model for research computing based on the Research Computing 2030 task force recommendations. A new five-year Memorandum of Understanding unifies university efforts to coordinate research computing across all campuses and units, emphasizing integration, efficient use of resources, financial sustainability, strong researcher support, and equitable access. This commitment will establish a research computing environment that enables interdisciplinary collaboration, increases capacity, and evolves alongside changing research requirements to support long-term competitiveness.

  OSU will establish a governance framework to guide policy development and ensure strong faculty participation and researcher input. This structure will distinguish high level strategic governance from operational decision-making for research computing systems. Additionally, the framework will include bilateral Memorandums of Understanding between the Division of Research and Innovation, University Information and Technology, and units providing research computing services. These agreements will formalize roles, responsibilities, and ongoing commitments related to funding, infrastructure, staffing, and services.

  As the Jen-Hsun Huang and Lori Mills Huang Collaborative Innovation Complex nears completion, the Division of Research and Innovation and University Information and Technology are collaborating to establish the infrastructure necessary to support OSU's incoming supercomputer. These efforts include the coordination of several working groups and task forces to implement and oversee the foundational elements necessary for the supercomputer's integration, including sufficient and sustainable cooling and power, scalable data storage, regulatory compliance, and advanced security. Recent accomplishments include the expansion of OSU's network capabilities to 400GB and an initiative to integrate storage systems specifically for data that is rarely accessed but still necessary to preserve for legal, regulatory, and/or historical reference. These efforts are progressing in alignment with the Huang Complex's construction timeline.

STRENGTHENING THE INFORMATION SECURITY PROGRAM

The Office of Information Security leads the university's information security program, which is based on the National Institute of Standards and Technology, Cybersecurity Framework. In early 2024, the institute released and updated framework, introducing significant changes. The most notable change was the addition of a Govern function to the existing five functional areas (Identify, Protect, Detect, Respond, Recover).

In the 2025 maturity review of the OSU Information Security Program, the largest improvement area was in Governance, reflecting a 4% improvement from 2024. The improvement was driven by the development of cybersecurity risk appetite statements, targeted actions to address increased Department of Defense compliance requirements for contract and research activities, and the development of improved processes and practices for policy development as well as balancing business needs and cybersecurity risks. Modest improvements in Identify (1.24%)

and Detect (1.92%) were realized through maturing and expanding AI use in cybersecurity defense and the move of key administrative systems to the State of Oregon Data Center.

Progress Report

Major Program achievements over the last year include:

- Gramm-Leach-Bliley Act Safeguard Rule: Compliance was confirmed by the 2025 external Annual Financial Audit.
- The Security Operations Center safeguards approximately 100,000 accounts, leveraging real-time insights to address vulnerabilities before they can be exploited. Since 2022, focused efforts have resulted in a remarkable 78.84% reduction in compromised accounts, underscoring the effectiveness of an integrated approach and the vigilance of the OSU community.
- Two new unit-level rules went into effect this year. The Baseline Standards of Care rule establishes minimum security standards for all OSU workstations and servers, strengthening the university's overall security posture. The Controlled Unclassified Information rule provides clear guidance for researchers and administrative units on properly handling, supporting compliance and protecting sensitive information.
- Partnering with the Division of Research and Innovation to support high-compliance research requirements, improve grant competitiveness and meet evolving research compliance requirements. OSU has contracted services with UC San Diego to meet the US Department of Defense Cybersecurity Maturity Model Certification Level 1 (Federal Contract Information) and Health Insurance Portability Accountability Act compliance requirements. The Division of Research and Innovation and University Information and Technology leadership are now evaluating options for achieving the US Department of Defense Cybersecurity Maturity Model Certification Level 2 (Controlled Unclassified Information) at OSU.
- On March 6, 2026, the OSU Data Security Incident Response Team conducted a tabletop exercise with the Ocean Observatories Initiative security team to test process and procedures necessary to respond to a simulated security incident in a major research program.

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

- Oregon State University is preparing for new Americans with Disabilities Act Title II requirements taking effect in April 2026. In partnership with the Disability Action Steering Group and campus stakeholders, University Information and Technology is leading a university-wide effort focused on accessible web and mobile content, video captioning, instructional materials, accommodations, and procurement practices. A new digital accessibility resource hub now provides guidance, training, and tools to support compliance. Recent web migrations enabled a comprehensive accessibility review, helping streamline content and raise OSU's overall website accessibility score to 80% as of October 2025, with automated scans showing 97.5% error-free pages. These improvements reflect strong campus collaboration and a shared commitment to digital inclusion. University Information and Technology also worked with Kaltura to enable

auto-captions on all new university videos, supporting upcoming ADA requirements and reinforcing OSU's dedication to accessible learning environments.

- The IT Expense Optimization Task Force, convened in April 2025, was charged with simplifying IT processes and reducing administrative complexity while continuing to support the university's academic and research missions. The task force developed a university wide operational framework to guide IT procurement, improve consistency, strengthen security compliance, and reduce costs. The working group's report and recommendations were delivered to the Provost and VP/CIO on December 1, 2025, and identify significant opportunities for immediate efficiencies and financial savings.

- Community Engagement – Cybersecurity Awareness Month 2025 events included a cybersecurity carnival on the Memorial Union Quad, a keynote presentation on cyber intelligence, an FYI Friday event, and engagements at OSU-Cascades and Hatfield Marine Science Center.

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

IDENTITY AND SMART ACCESS

Grounded in the principles of the Cybersecurity and Infrastructure Security Agency Zero-Trust Maturity Model, the Smart Access Program is enhancing the IT infrastructure across five key pillars: identity, endpoint, network, application, and data. Adopting zero-trust principles, conditional access policies have been applied to enhance authentication services, and additional policies are being developed to support device security.

Progress Report

Major Program achievements over the last year are listed below:

- Aligned the Identity and Governance Administration to Workday integration with the university's one digital identity strategy, establishing an authoritative system for identity correlation across the institution.

- Updated OSU's password policy, removing routine password changes for most users while relying on Duo Multi-Factor Authentication and modern monitoring to detect compromised accounts. Regular password updates will still be required for systems that protect the university's most sensitive data.

- Following Microsoft's end of support for Windows 10, the Office of Information Security partnered with the campus community to ensure a smooth and secure transition to Windows 11. This initiative involved assessing all Windows 10 devices, preparing units for potential budget impacts, and developing contingency strategies and guidelines to minimize operational disruptions.

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

EMERGING RISK AREAS

Emerging areas of technological, compliance and cyber risk have increased and are incorporated into the IT Roadmap.

Technology and Compliance

- OSU's expansive and diverse Internet of Things ecosystem spans research, facilities and operational technologies, requiring a coordinated approach to reduce institutional risk. In 2023, the OSU Energy Center underwent an assessment by Cybersecurity and Infrastructure Security Agency, which produced several recommendations, including the need to provide incident visibility into the protected Internet of Things environment. To advance these recommendations, OSU will conduct a proof of concept to determine whether current deployed families of cybersecurity tools can operate effectively within the Energy Center's environment. If successful, this approach will be scaled to additional segments of the OSU Internet of Things fleet, forming the foundation for a broader institutional security capability.

- Federal IT compliance requirements are on the rise. In late 2023, the US Department of Education mandated that certain data elements of the Free Application for Federal Student Aid be treated as Controlled Unclassified Information. Additionally, the US Department of Defense Cybersecurity Maturity Model Certification requirements came into effect on November 10, 2025, increasing compliance obligations for research funded by the Department of Defense. In January 2025, the National Institutes of Health issued updated guidance strengthening data security requirements for research involving controlled-access genomic data. The revised Genomic Data Sharing Policy now requires compliance with NIST SP 800-171 cybersecurity standards. OSU will align all high-compliance administrative and research environments with these controls to provide a consistent set of inherited safeguards and reduce the need for customized solutions.

- In spring 2024, the Department of Justice released a new rule under Title II of the Americans with Disabilities Act that requires the university to meet certain web and mobile technical standards by April 24, 2026. Adhering to these regulations is not just a legal requirement but a proactive step towards upholding the rights of individuals with disabilities. OSU has a large backlog of inaccessible documents that are difficult to locate, prioritize, and remediate. A consistent document lifecycle strategy is needed to determine which materials should be retired, converted, or fully remediated. Course materials also pose significant accessibility risks due to varied practices and limited support. Without clear university wide standards, accessibility depends on individual effort, leading to uneven student experiences, more accommodation needs, and higher compliance risk.

Cybersecurity

- Microsoft's Digital Defense Report 2025 indicates that the Research and Academia sector remains a top target for threat actors due to its high value intellectual property, decentralized infrastructure and expansive digital footprint. Nation-state activity is substantial with 14% of all nation-state level attacks focused on the Research and Academia sector. The report highlights increased use of AI for sophisticated cyber-attacks and social engineering campaigns. In response, OSU has spent the last several years strengthening defenses against identity-based threats. The Smart Access

Program will continue to expand protections across devices, applications (including AI) and data while also exploring opportunities to utilize AI in the university's cyber defense strategy.

NEXT STEPS

At its March 12 meeting, the Executive, Audit and Governance Committee will review the risk management report with staff and may identify additional follow-up actions, as needed.

ATTACHMENT 1

Oregon State University
Enterprise Risk Management 2025 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	Establish a robust cybersecurity framework based on NIST that provides protection of sensitive data, maintains the integrity of our IT infrastructure, and fosters a culture of security awareness among all stakeholders. Our goals include implementing advanced security measures, conducting regular risk assessments, and providing continuous education and training to mitigate potential threats and vulnerabilities.	Operational, Compliance, Financial, Reputational	Provost, Vice Provost and Chief Information Officer, College Deans	Accept, Reduce, Share/Insure	Chief Information Security Officer; Chief Data Officer; Chief Technology Officer; Executive Director, Business Architecture; IT Security Advisory Committee

[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: next iteration • Develop update to charter • Publish standard processes • Review and update data management policy • Audit and document exiting data definitions • Implement centralized capability for Data Catalog, Dictionary, and Lineage for all data within OSU Data Platform • Develop Data Roadmap b. OSU Data Platform • Continue to add enterprise data pipelines to increase data available for analysis • Deprecate legacy data platforms • Release priority OSU data domain models that are aligned to the data dictionary and provide standard and consistent access to OSU data	**Completed and Planned Activities** a. Data Governance • Data stewards are active and meeting monthly at a minimum. • Data Governance charter is in progress • Multiple data governance processes are under development • Data definition prioritization and additional of essential new values within student domain is underway • Engagement with Microsoft underway to implement tooling for centralized data definitions, catalog, and lineage. • OSU Data Policy review and update is in progress, expected before June 2026. b. OSU Data Platform • CDO 100-day report is complete. Data roadmap development is underway. • Migration away from 1 of 9 data environments has been declared and is underway. This will result in the consolidation of significant student data into OSU Data Platform and set the stage for platform deprecation in November 2026. • Successful publishing of multiple strategic dashboards and reports including First Year Registration and Retention (FYRR), PWS planning, College Research Award, Student Achievement and Mission Fulfillment, Accreditation. • Launch of Boomi as new integrations platform for OSU planned for March in support of Workday go-live.

OBJECTIVE 2: Strengthening OSU's Information Security Program	
Actions to Satisfy Objective	**Status Report**
Information Security Program **Govern** 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. Develop Risk appetite statements. c. Complete Organizational Profiles. d. Publish and update information security rules. **Identify** a. Improve asset management program. b. Mature vulnerability program c. Improve incident response plans. **Protect** a. Continue to mature identity service. b. Mature awareness and training program. c. Update and replace out of support systems. **Detect** a. Expand continuous monitoring. b. Sustain and improve continuous monitoring. **Respond** a. Mature the incident management system. b. Improve response within OSU IT community. **Recover** a. Document system recovery requirements.	**Completed and Planned Activities:** **Govern** a. Resilience Plan and Roadmap being finalized. b. Risk Appetite statements complete. c. CISO briefed to ISAC approach to maintain one IT Organizational Profile for now. Potential profiles for AI and IoT under consideration. d. Two information security rules published in 2025. **Identify** a. Implemented ITSM Tool. ITSM tool offers potential for better tracking of IT assets b. Hired a vulnerability analyst; improved internet facing risk posture. c. Cyber Tabletop exercise in March 2026 that reviewed response for research programs. **Protect** a. 78% reduction in compromised accounts since 2021. b. Annual training for UIT system administrators. c. Windows 11 project complete. **Detect** a. Improve automation, integration of AI and expand to AMP data sources. b. Continuous monitoring and detection processes in place and constantly improved. **Respond** a. Incident response documentation published, and incident commander qualification process is in place. b. Planning exercises to involve OSU IT community in incident response. **Recover** a. Business Continuity and Disaster Recover Rule published and Business Impact Analysis documentation underway for key systems.

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. Device and Identity Management c. Zero Trust Architecture	**Completed and Planned Activities:** a. Fielded. Current work is on-boarding new applications and improving role-based access controls. b. Device and identity services improved, including monitoring of identities and devices as well as identity and device controls. c. Basic ZTA is enabled. Continuous improvement following the CISA Zero Trust Maturity Model.

Performance Metrics		
Build a robust and unified university data/information ecosystem that delivers data as a strategic working asset		
Goal	**FY2026 Status**	**Comments**
Deliver actionable information for university leaders. Create Strategic Dashboards and Tools for Leadership and key stakeholders. Transform all public facing institutional reports into actionable dashboards.	Data Platform: • Developed enterprise data pipelines and modeled key data domains (Complete) • Student data migration (in process) Strategic Dashboards: • First-Year Registration and Retention (Complete) • College Research Award (Complete) • Student Achievement and Mission Fulfillment (Complete) • AAU (Complete) Public Facing IR • OSU 2025 Accreditation Dashboard has been published for the first time as an interactive public dashboard. https://academicaffairs.oregonstate.edu/academic-operations/student-achievement-and-mission-fulfillment-dashboard	Initial set of dashboards delivered and are continually improved. Tasks need to support AMP program underway, such as data transformation work and report design. Further work on the public facing institutional dashboards into interactive dashboards is planned work after the consolidation of data into OSU Data Platform slated for early FY27.

OSU CSF Risk Profile for Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) systems and data (Administrative zone)		
Goal	**FY2026 Status**	**Comments**
Govern: 3.17 Identify: 3.46 Protect: 3.4 Detect: 3.4 Respond: 3.48 Recover: 3.33	Govern: 2.48 Identity: 2.68 Protect: 2.59 Detect: 2.81 Respond: 2.85 Recover: 2.72	New baseline based on NIST CSF 2.0. Score rubric is based on: • Tier 0: None • Tier 1: Partial • Tier 2: Risk Informed • Tier 3: Repeatable • Tier 4: Adaptive
Deliver training and resources to employees		
Goal	**FY2026 Status**	**Comments**
100% participation in employee and student worker training. Awareness and Training is a key element of the NIST CSF Protect functional area.	Delivered 77% of Staff and 38% of student employees as of February 6, 2026. Cybersecurity Awareness Month engaged several hundred students at the Cybersecurity Carnival, and about 500 employees at training and awareness events. OIS participated in the Library's Privacy Day in January 2026, engaging over 100 students.	Information Security is an annual training requirement. HR has implemented an escalation process for non-compliant employees. Training videos updated for this year. Controller Unit had Cybersecurity Training for entire unit during FY26.
Protect Oregon State University information assets and stakeholder privacy in line with university values		
Goal	**FY2026 Status**	**Comments**
Manage all OSU Identities consistently Mature Identity Practice Manage all OSU owned devices consistently	All OSU Network ID (ONID) accounts are managed in a central tool Verified all identities with elevated permissions, removed unnecessary accounts Transitioned authentication to the cloud and continued to improve Multifactor security.	Identity Governance and Administration tool process improvements (aided by internal IT Audit) Passwordless authentication is long-term goal for OSU Marked drop in large scale phishing attacks.