BOARD OF REGENTS OF THE UNIVERSITY OF WISCONSIN SYSTEM

Audit, Risk, and Compliance Committee

Thursday, December 4, 2025
10:45 a.m. – 12:00 p.m.

Room 275A, 2nd Floor
James R. Connor University Center
190 Hamilton Green Way, Whitewater, Wisconsin
& By Videoconference

A. Calling of the Roll

B. Declaration of Conflicts

C. Proposed Consent Agenda:
   1. Approval of the Minutes of the September 18, 2025, Audit, Risk, and Compliance Committee Meeting
   2. Office of Internal Audit: Fiscal Year 2026 Audit Plan Progress Report
   3. Office of Internal Audit: Results of Reports Recently Issued

D. Office of Compliance and Risk Management
   1. Progress Report on UW System Administrative Policy (SYS) 625 Youth Protection Audit

E. Office of Information Security
   1. Cybersecurity and Privacy Risks Related to the Use of Generative AI

F. Move into closed session to:
   1. Consider strategies for crime detection and prevention, as permitted by s. 19.85(1)(d), Wis. Stats.

OFFICE OF INTERNAL AUDIT
FISCAL YEAR 2026 AUDIT PLAN PROGRESS REPORT

REQUESTED ACTION

For information and discussion.

SUMMARY

One of the responsibilities of the Audit, Risk, and Compliance Committee, as outlined in the committee charter, is to review and approve the annual internal audit plan and receive interim progress reports at least quarterly.

The attached chart provides a summary of audit progress for the Fiscal Year 2026 Audit Plan.

Presenter(s)

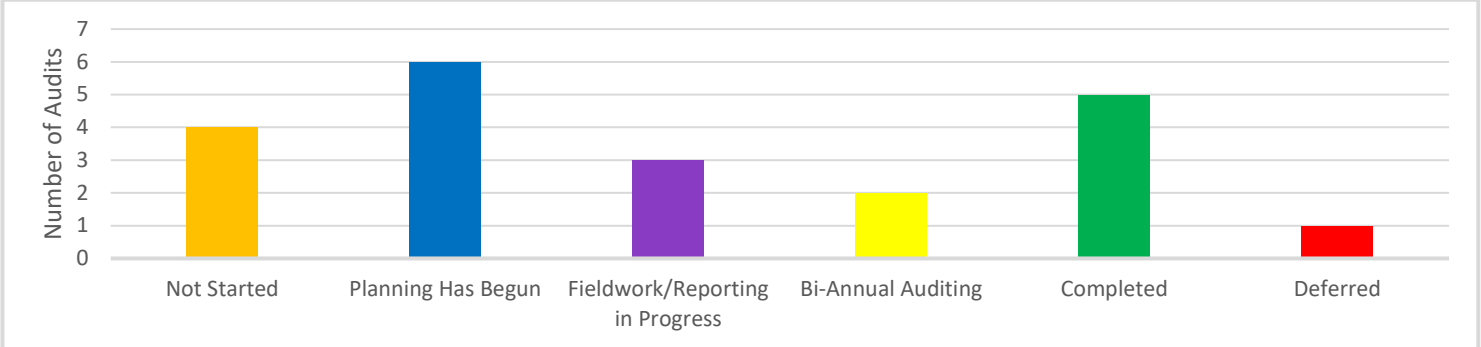
- Lori Stortz, Chief Audit Executive

ATTACHMENTS

A) Universities of Wisconsin Office of Internal Audit Fiscal Year 2026 Audit Plan Progress Chart.

OFFICE OF INTERNAL AUDIT
FISCAL YEAR 2026 AUDIT PLAN PROGRESS

	Title	Risks
1	Payroll (Bi-Annual Auditing)	Fraud, Data Accuracy, Compliance with Policy
2	Purchasing Cards (Bi-Annual Auditing)	Fraud, Embezzlement, Compliance with Policy
3	$31.89M Funding in Biennium for Workforce Devel. 4 High-Demand Areas	Reputational, Compliance
4	Budgetary Controls at UW-Madison	Fraud, Compliance, Reputational
5	Commitments Made by System to WI Legis. per BOR Resol. Dec. 13, 2023	Reputational, Compliance
6	Cybersecurity	Data Security, Fraud, Operational, Compliance with Policy
7	Employee-Owned LLC's Contracting with Universities	Conflicts of Interest, Financial, Youth Protection
8	Information Technology (IT) Distributed Units	Data Security
9	Institutional Relationships with Foundations and Associated Affiliated Organizations	Fraud, Reputational, Compliance with Policy
10	Internal Assessment Fiscal Year 2025	Conformance with Institute of Internal Audit (IIA) *Standards*
11	Internal Assessment Fiscal Year 2026	Conformance with Institute of Internal Audit (IIA) *Standards*
12	Physical Plant Services Chargebacks	Financial, Compliance with Policy
13	Research Administration Management Portal (RAMP)	Data Security, Operations, Compliance with Grant Requirements
14	Segregated Fees	Financial, Compliance with Policy, Reputational
15	Shared Services (Excludes UW-Madison)	Compliance, Operational
16	Third-Party Risk Management	Operational, Financial, Reputational, Data Security
17	Workday Go Live, Key Controls and Business Processes	Data Security, Operations, Financial
18	NCAA Athletics Division I Agreed-Upon Procedures Engagements	Compliance with NCAA Agreed-Upon Procedures
19	NCAA Athletics Division II Consulting Project	Compliance with NCAA Agreed-Upon Procedures
20	Office of Educational Opportunity (OEO)	Compliance
21	Wisconsin Educational Development Corporation (WEDC) Grants	Grant Compliance, Fraud



Bar graph reflects the number of audits per stage of completion, with various stages on the x-axis and the number of audits on the y-axis. Not Started 4 audits, Planning Has Begun 6 audits, Fieldwork/Reporting in Progress 3 audits, Bi–Annual Auditing 2 audits, Completed 5 audits, Deferred 1 audit.

OFFICE OF INTERNAL AUDIT
RESULTS OF REPORTS RECENTLY ISSUED

REQUESTED ACTION

For information and discussion.

SUMMARY

Since the September 18, 2025, meeting of the Audit, Risk, and Compliance Committee, the Office of Internal Audit has issued the following report:

- Office of Educational Opportunity (OEO) Audit - Executive Summary

Presenter

- Lori Stortz, Chief Audit Executive

BACKGROUND

One of the responsibilities of the Audit, Risk, and Compliance Committee, as outlined in the committee charter, is to summarize results of reports recently issued.

OFFICE OF COMPLIANCE AND RISK MANAGEMENT PROGRESS REPORT ON UW SYSTEM ADMINISTRATIVE POLICY (SYS) 625 YOUTH PROTECTION AND COMPLIANCE AUDIT

REQUESTED ACTION

For information and discussion.

SUMMARY

The Universities of Wisconsin Office of Compliance and Risk Management (OCRM) will provide a general update on its progress made in in response to the UWSA Management Letter issued on May 16, 2025, related to the *SYS 625 Youth Protection and Compliance Audit*.

Presenter

- Paige Smith, Chief Compliance and Risk Officer

BACKGROUND

In accordance with its 2025 Audit Plan, the Office of Internal Audit performed an audit of high-risk areas of UW System Administrative Policy 625, Youth Protection and Compliance (SYS 625). The audit evaluated and tested covered activities subject to SYS 625 at all 13 UW universities between the activity period from June 1, 2024, through November 30, 2024. The audit included a review of UWSA's activities under SYS 625, resulting in a UWSA Management Letter issued May 16, 2025.

ATTACHMENT

A) OCRM Progress Report on SYS 625 Youth Protection and Compliance Audit

SYS 625 Audit: UWSA Management Letter
Office of Compliance and Risk Management
Progress Chart

Topic	Planned Course of Action*	Audit Comment	Status/Progress
Leadership and University Engagement	Meet with university leader(s) to review audit findings and ensure that management responses are being completed within timelines set by **August 31, 2025.** Schedule "check-in" compliance meetings with identified university leaders and Pre-College Liaisons (PCL) to review compliance under SYS 625.	Comment 1: Monitoring of Youth Protection Activities	**Completed**: Initial meetings have occurred with all 13 university leaders and stakeholders. **Completed**: OCI met with leadership (or designees) for all 13 universities in November 2025. Additional meetings will occur in spring of 2026.
SYS 625 Policy Review	Meet with pertinent stakeholders and conduct initial reviews of SYS 625 and RPD 20-19 for potential edits to address audit findings and concerns by **August 15, 2025.** Submit formal SYS 625 policy revision recommendations to President Rothman and university stakeholders for consideration on or before **March 1, 2026.**	Comment 3: SYS 625 Policy Clarifications and Guidance Comment 4: Criminal Background Check Databases	**Completed:** Meetings have occurred with pertinent stakeholders on SYS 625. **Completed:** A proposed revision to SYS 625 has been shared with President Rothman and university stakeholders. The proposed revisions will be submitted to the UWSA policy committee by November 21, 2025, for formal review and approval on or before March 1, 2026. Revisions to RPD 20-19 will be considered only if necessary.

Mentoring and Support	Develop a plan for offering additional support, depending on the type of training or expertise sought by **August 30, 2025.** Secure membership to Higher Education Protection Network (HEPNet) (national youth protection and safety organization) for universities.	Comment 2: Youth Protection Resources and Training	**Completed:** OCI has met with each PCL to identify specific training and mentoring needs. Responses have been used to determine additional support. Additional training on data software has been provided to PCLs to assist in their data and compliance tracking. **Completed:** OCI has secured a HEPNet membership.
Third Party Agreements/Records Management	Collect and review a sample of third-party agreements including terms and conditions for emergency management plans and insurance requirements by **September 15, 2025**. Review university-level record management processes for collecting and maintaining all third-party agreements.	Comment 3: SYS 625 Policy Clarifications and Guidance	**Completed:** Documents have been spot-checked on a regular basis for a handful of universities. Universities have improved their record-keeping processes per their audit findings.
Training	Create training program on SYS 625 compliance requirements for use by leadership, PCLs and program directors on or before **September 15, 2025**,	Comment 1: Monitoring of Youth Protection Activities	**Completed:** A SYS 625 compliance training program was provided to universities through live, virtual sessions in November 2025. The training program is also available for use by university precollege liaisons at their own discretion.
Compliance Monitoring	Conduct regular monitoring and assessment of university actions regarding compliance with audit findings and management letters. Identify and address gaps in compliance, including screening and training completions for volunteers, retaining executed third-party agreements. Notable concerns will be shared with university leadership for consideration. Complete by **September 30, 2025.**		**Completed:** OCI is conducting regular compliance monitoring for select universities. If a compliance gap is identified, OCI will meet with the university to address the issue promptly.

Data Tracking	Evaluate existing software for program activity tracking, registration and compliance requirements by **October 30, 2025.** Recommend existing contracts be renewed or other services by **February 15, 2026.**	Comment 2: Youth Protection Resources and Training	**Completed:** OCI has evaluated software for SYS 625 data tracking and compliance monitoring. The information has been shared with chief business officers for consideration. **In Progress:** Final decisions on necessary software will be made on or before February 15, 2026.

*This chart is intended as a high-level overview by relevant topic of the UWSA Management Letter and additional compliance efforts. The noted comment sections as referenced in the chart can be found, in part, below per the UWSA Youth Protection and Compliance Audit Management Letter.

Key

Completed
In Progress
On Hold

*SYS 625 AUDIT: UWSA MANAGEMENT RESPONSE LETTER

Recommendations and Management Responses

COMMENT 1: Monitoring of Youth Protection Activities

Audit Recommendation:
We recommend UW System establish a formally defined training and monitoring practice to periodically review universities' data and third-party agreements to ensure compliance with SYS 625.

We recommended to universities that they establish a process for risk management to review and approve third-party insurance coverage. Additionally, given the importance of proper third-party contracts and the related insurance coverage, UW System should consider how they can help the universities manage this activity or provide additional support to universities' risk management authorities.

UWSA Management's Response:
Planned course of action: On or before **August 31, 2025**, the Office of Compliance and Integrity (OCI) will collaborate with other UWSA offices to identify specific areas of SYS 625 training that are not otherwise provided and in response, develop said trainings for Precollege Liaisons (PCLs) and university stakeholders to ensure universities are informed and aware of their SYS 625 compliance requirements and opportunities for improvement.

On or before **August 31, 2025**, and based on needs and input of PCLs and university stakeholders, OCI will develop and/or procure relevant training programs, including the option of purchasing training programs or webinars through HEPNet resources.

On or before **September 30, 2025**, OCI will collaborate with university stakeholders to review SYS 625 requirements related to third-party agreements, including whether improvements are needed to review and approve necessary third-party documentation, including insurance coverage and emergency management plans, as applicable.

On or before **September 30, 2025,** and in collaboration with university leadership, OCI will implement a centralized compliance monitoring process related to tracking relevant data, including screening and training completions for volunteers, retaining executed third-party agreements. The work will continue throughout the FY25-26 fiscal year with a completion date for all 13 universities on or before **May 1, 2026**. OCI will provide an update to President Rothman and ARC Chairs on or before **June 30, 2026**.

COMMENT 2: Youth Protection Resources and Training

Audit Recommendation:
Collaborate with each PCL to understand how their role fits into their university's governance structure, along with any challenges the PCL experiences in getting the university to embrace the compliance requirements of SYS 625 and university processes. This may result in opportunities for UW System to recommend to the universities opportunities to realign the PCL role in the governance structure to reinforce the authority of the PCL and facilitate better compliance.

Coordinate with the universities to establish enhanced support structures for PCLs. This should include an evaluation of opportunities to assist the universities and their PCLs with onboarding and mentoring for those individuals that are new to the role.

Offer targeted, topic-specific training sessions to further develop the skills and capabilities of PCLs.

Consider whether a systemwide membership to the Higher Education Protection Network (HEPNet) can be purchased for the benefit of all universities.

Evaluate the feasibility of consolidating current software systems into a single, integrated platform to reduce manual data entry and improve operational efficiency.

UWSA Management's Response:
On or before **August 30, 2025**, the Compliance Specialist for Youth Protection will meet with each PCL to collaborate on their current roles, review their audit findings, and identify specific training, mentoring and/or onboarding needs. OCI will develop a plan for providing additional support, depending on the type of training or expertise sought.

OCI will retain its HEPNet membership and seek opportunities to invite PCLs and other stakeholders to trainings, webinars and other learning opportunities, including sharing of written materials and resources. OCI will also research opportunities for securing a systemwide membership for all 13 universities.

The current database software platforms available to all universities are up for renewal during FY26-27. During the 25-26 academic year, OCI will work with universities to determine whether these remain the most useful and cost-efficient options at a systemwide level. OCI will also continue to search for other opportunities to secure one database platform that would fulfill all the compliance data tracking requirements under SYS 625. On or before **March 30, 2026**, UWSA will provide viable alternatives for universities to consider by the time the existing Youth Activity Registration System (YARS) expires in May 2026.

Starting in the fall semester of 2025, the Chief Compliance and Risk Officer, along with the Compliance Specialist for Youth Protection, will schedule at least one meeting per semester with university leadership (or designee), PCL and their supervisor to review their existing compliance efforts under SYS 625, identify and discuss any best practices and reporting structures for the PCL role, evaluate any existing compliance gaps, collaborate on a course of action to address said gaps, and offer additional OCI support, as necessary and within its capacity.

Unless otherwise noted above, OCI will begin the planning process for the above actions and take steps to complete each task within a reasonable period of time, but no later than **December 31, 2025**.

COMMENT 3: SYS 625 Policy Clarifications and Guidance

Audit Recommendation:
We recommend UW System consider how either modifications to SYS 625 or additional guidance may help clarify the observations noted above. Additionally, UW System should modify SYS 625 to ensure it reflects any additional requirements written in the frequently asked questions section of the policy.

UWSA Management's Response:
OCI will initiate a review of SYS 625, in collaboration with the Office of General Counsel, Office of Risk Management, PCLs and other university stakeholders, to evaluate notable sections of the policy that should be revised with the goal of maintaining appropriate and reasonable standards for the overall safety and protection of youth during covered activities. This work will include an update of the FAQs to ensure consistency and usefulness.

OCI will schedule initial meetings with pertinent individuals by **August 30, 2025,** and develop a strategic plan for this work with timelines and deliverables with the goal of having formal policy revision recommendations to President Rothman and university stakeholders for consideration on or before **March 1, 2026.**

COMMENT 4: Criminal Background Check Databases

Audit Recommendation:

We recommend UW System collaborate with the Board of Regents Office to amend RPD 20-19 for current practices or adjust the standard background check package to include the required databases.

UWSA Management's Response:

OCI will collaborate with Office of Human Resources, Office of General Counsel, and Board of Regents Office to review the existing language and recommend policy revisions, if needed, to match existing practices and/or level and type of background checks necessary to adequately screen volunteers who seek to participate in a covered youth activity.

An assessment of RPD 20-19 will be initiated on or before **August 15, 2025**, and be completed with recommendations to President Rothman and Regent leadership on or before **November 30, 2025.** Depending on whether a policy revision is recommended, this work should be completed on or before **June 30, 2026.**

For Internal Use Only

CYBERSECURITY AND PRIVACY RISKS RELATED TO THE USE OF GENERATIVE AI

REQUESTED ACTION

For information and discussion.

SUMMARY

The Universities of Wisconsin must weigh the innovation and efficiency gains of Generative AI against its risks. This discussion aims to examine the fundamental causes and possible implications of cybersecurity and privacy risks related to Agentic AI and Shadow AI.

Definitions

- **Generative AI:** AI systems that can create new content, such as text, images, audio, or code, by learning patterns from large datasets.
- **Agentic AI:** AI systems designed to take actions or make decisions autonomously, often capable of completing multi-step tasks without continuous human direction.
- **Shadow AI**: AI tools, services, or models used within an organization without formal review, approval, or visibility.

Presenter

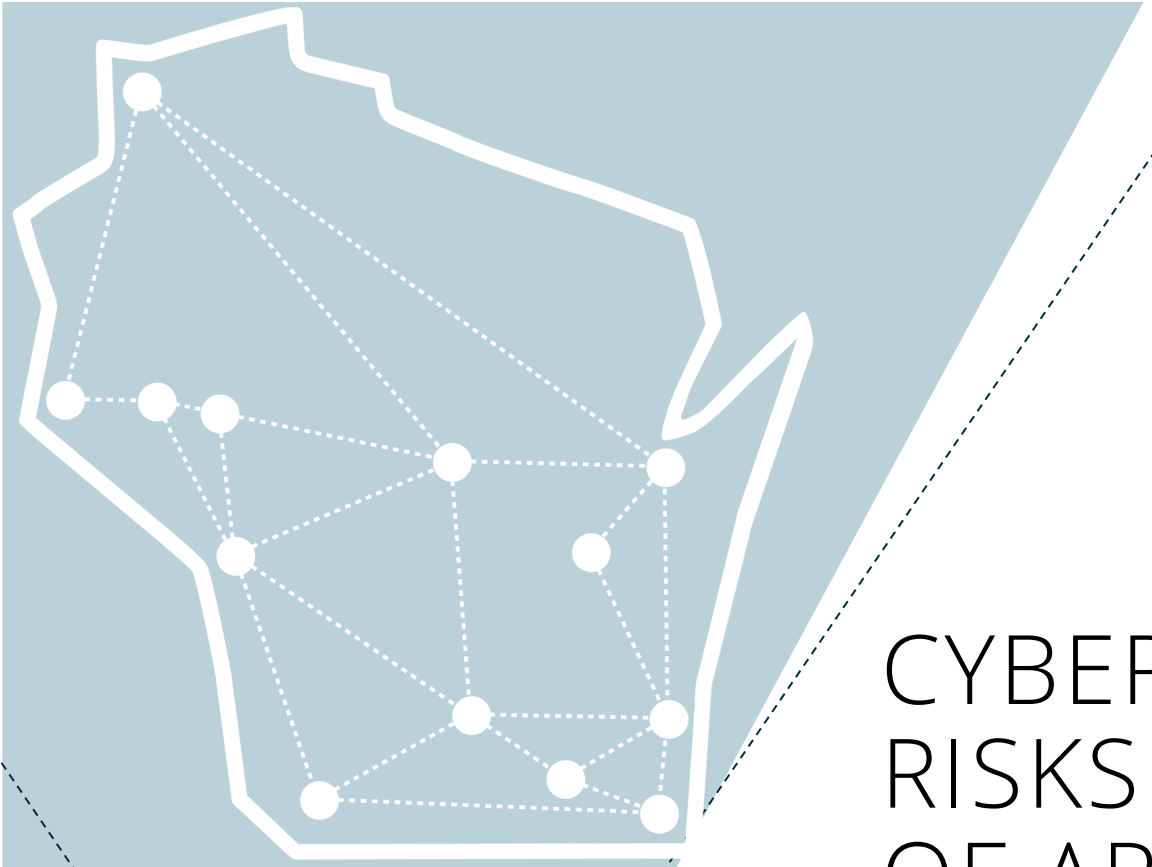
- Edward Murphy, Associate Vice President, and Chief Information Security Officer

BACKGROUND

The technology environment at the Universities of Wisconsin comprises a blend of contemporary and legacy systems. Universities of Wisconsin campuses experience frequent cyberattacks. The education and research sector remains a prominent target for both cybercriminals and nation-state actors, whose objectives include disrupting operations, stealing proprietary information, and pursuing financial gain through extortion.

ATTACHMENT

A) Cybersecurity and Privacy Risks Associated with the Use of Artificial Intelligence.



UNIVERSITIES OF WISCONSIN

CYBERSECURITY AND PRIVACY RISKS ASSOCIATED WITH THE USE OF ARTIFICIAL INTELLIGENCE

Edward Murphy, Associate Vice President and CISO

AI UNIVERSE

DALL·E

Fitness Bands with AI Coaching

Sora

AI Hearing Aids

Dia

Perplexity Comet

Smart Glasses with GPT

GitHub Copilot

ChatGPT Atlas

AGENTIC AI

- Web Browsers
  - ChatGPT Atlas
    - Features agent mode
  - Perplexity Comet
    - Built for research and automating tasks
  - Dia
    - Proactive agentic browser equipped with adaptive memory

- Possible applications
  - **Faculty**: Streamline LMS tasks such as uploading syllabi and posting announcements.
  - **Students**: Generate summaries of lecture recordings and develop flashcards.
  - **Staff**: Manage meeting schedules, arrange flights, and edit documents.

AGENTIC AI RISKS

Cybersecurity Threats

Agentic AI systems can expose campuses to data breaches and unauthorized access, compromising sensitive institutional information.

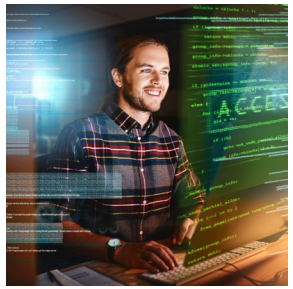
Privacy Risks

AI interactions may lead to inadvertent sharing of personal or academic data, threatening student and faculty privacy.

Context Poisoning

Attackers embed hidden or misleading instructions in content read and interpreted by Agentic AI browsers, tricking the AI into executing actions that compromise security or privacy.

SHADOW AI RISKS

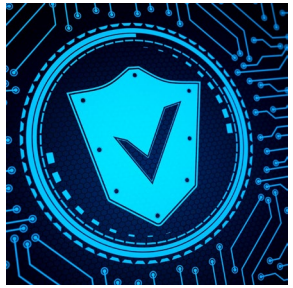


Lack of Visibility and Control

Shadow AI involves artificial intelligence tools that are deployed without IT department approval or oversight, increasing institutional risks.

Data Privacy Breaches

Sensitive student and research data may be exposed due to unmonitored AI tools, creating significant privacy concerns.



Cybersecurity and Compliance Risks

Shadow AI increases vulnerability to cyberattacks and may lead to violations of data regulations such as FERPA.

MITIGATING AI RISKS

AI Governance and Policies

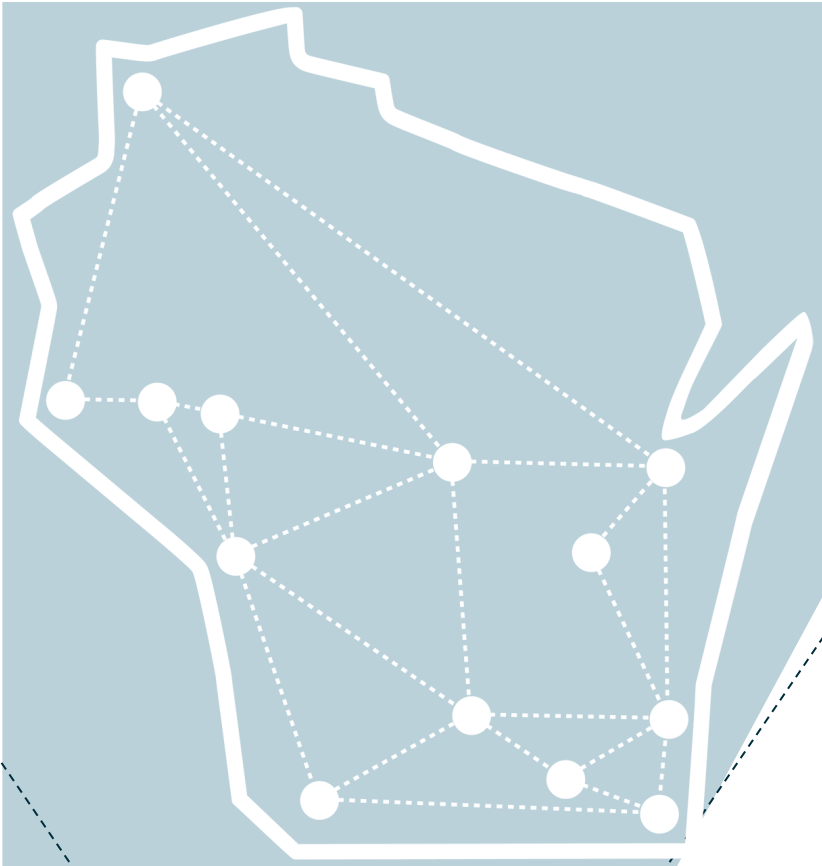
Effective AI governance ensures transparent, accountable use of AI systems across university environments. Includes security risk assessments.

Promote AI Literacy

Faculty, staff and students are educated on secure AI tool use and protecting data privacy, promoting responsible technology adoption.

Monitoring and Cybersecurity

Robust monitoring systems detect unauthorized AI use, minimizing cybersecurity threats and protecting sensitive university information.



UNIVERSITIES OF WISCONSIN

THANK YOU

Edward Murphy, edward.murphy@wisconsin.edu