



# Audit & Compliance Committee

April 2026

April 9, 2026

Approximately 15 minutes following adjournment of Finance & Operations Committee

Campus View Room, McNamara Alumni Center

## AUD - APR 2026

### 1. University Compliance Landscape Analysis

Docket Item Summary - 3

Compliance Landscape Analysis Recommendations - 5

Presentation Materials - 14

### 2. Enterprise Risk Management and Institutional Risk Profile

Docket Item Summary - 25

Presentation Materials - 27

### 3. Information Items

Docket Item Summary - 41

External Auditor Review And Summary Of External Auditor Relationships  
And Services Provided - 43



# BOARD OF REGENTS DOCKET ITEM SUMMARY

---

**Audit & Compliance**

**April 9, 2026**

**AGENDA ITEM:** University Compliance Landscape Analysis

**Review**

**Review + Action**

**Action**

**Discussion**

*This is a report required by Board policy.*

**PRESENTERS:** Gregg Goldman, Executive Vice President for Finance and Operations

## **PURPOSE & KEY POINTS**

The purpose of this item is to provide an analysis of the University’s compliance landscape and to recommend next steps to strengthen the institution’s compliance framework.

This work reflects a proactive effort to modernize the University’s approach in response to an increasingly complex regulatory environment and evolving best practices across higher education. Peer institutions have similarly reassessed their compliance structures to ensure they are well-positioned to identify, coordinate, and manage risk in a more integrated and forward-looking way.

Compliance responsibilities at the University are broad and highly distributed, spanning academic, research, clinical, and administrative functions. This decentralized model enables strong subject-matter expertise and embeds compliance into day-to-day operations. The University’s compliance ecosystem is mature in many respects, with strong local expertise, committed professionals, and established processes in key areas. At the same time, the scale and complexity of regulatory requirements across multiple campuses, functions, and external partnerships create opportunities to strengthen coordination, transparency, and systemwide alignment.

The analysis highlighted that compliance activities are often managed effectively within individual units but are not always consistently connected across functions. In a complex environment, particularly in areas such as healthcare, research, and privacy, risks and compliance issues may span multiple domains, underscoring the need for a more coordinated, institution-wide approach that enables earlier identification of risk, improved information sharing, and more consistent oversight.

Several common themes emerged through stakeholder feedback, including opportunities to:

- clarify leadership, authority, and accountability for systemwide compliance oversight and management;
- strengthen governance structures to support coordinated oversight and decision making;
- establish a more unified approach to privacy and data security;
- improve coordination and communication across compliance functions and campuses;

- enhance infrastructure, including technology, training, and data management tools; and
- better define roles and responsibilities to improve alignment and efficiency.

After reviewing the University's current compliance framework, the following recommendations have been developed to strengthen the framework while preserving the benefits of a distributed model:

- establishing strengthened leadership for institutional compliance, including an expanded and elevated Chief Compliance Officer role;
- reinvigorating governance structures, including reestablishing an executive-level compliance oversight committee and strengthening policy governance;
- formalizing systemwide coordination mechanisms, including a rechartered Compliance Partners network, cross-functional affinity groups, and an Institutional Strategic Risk and Compliance Group to support risk identification and escalation;
- developing a more coordinated and comprehensive privacy and data security function;
- modernizing compliance infrastructure, including technology tools for training, reporting, and monitoring; and
- standardizing compliance training and onboarding to promote consistent understanding of responsibilities.

These recommendations are grounded in leading practices and are designed to create a more integrated, transparent, and proactive compliance framework that enhances the University's ability to identify and manage risk, meet regulatory obligations, and support its mission.

The presentation will provide additional detail on the current state and a proposed future-state framework and will outline a phased approach to implementation. Initial efforts will focus on advancing priority recommendations related to leadership, governance, and systemwide coordination. Additional recommendations will be further assessed and prioritized following the hiring of a new Chief Compliance Officer, allowing for their evaluation and input as part of the implementation strategy.

## **BACKGROUND INFORMATION**

The compliance landscape analysis was conducted in October 2025 following the organizational realignment of the Office of Institutional Compliance under the Executive Vice President for Finance and Operations. The purpose of the analysis was to document the current compliance environment, structure, roles, responsibilities, and levels of coordination. The review included engagement with compliance leaders and stakeholders across campuses and functional areas.

The Chief Compliance Officer provides annual Institutional Compliance and Conflict of Interest Reports to the Audit & Compliance Committee, with the most recent report presented in December 2025.

## **Compliance Landscape Analysis Recommendations**

Based on the Compliance Landscape Analysis project findings, several strategic recommendations have been developed to strengthen coordination, oversight, and consistency across the University's compliance environment. These recommendations address structural, operational, and cultural challenges identified through interviews and analysis. Together, they are designed to balance the University's decentralized strengths with greater systemwide alignment, building a more integrated, transparent, and proactive compliance framework that mitigates risk, fosters accountability, and embeds compliance as an institutional foundation.

Additionally, those interviewed in the project provided recommendations to improve the University's compliance program and related activities. These recommendations are listed at the end of this document.

### **Recommendations from Compliance Landscape Analysis**

#### **1. Strengthen Leadership for Institutional Risk and Systemwide Compliance**

Create a leadership function(s) for institutional risk and systemwide compliance strategy, oversight, and reporting.

Lead Office: EVPFO / OIC

Timeframe: Short-Term (6–12 mo.)

Establish a unified leadership function for institutional risk management and systemwide compliance strategy, oversight, and reporting. This should include expanding the Chief Compliance Officer's responsibilities, paired or aligned with a Chief Risk Officer or equivalent function, to ensure coordination between risk and compliance across the University.

The Chief Compliance Officer should be responsible for coordinating University-wide compliance, aligning policies, and prioritizing risks. Leading the OIC, the position should have clearly defined responsibilities and authority to coordinate and oversee compliance activities across the University. This includes establishing a central function to assess new laws and regulations, determine impact and resource needs, and guide implementation. Additionally, this senior compliance leader should be available as a trusted advisor to campus and unit leaders, providing consultation and judgment on complex or cross-functional compliance issues.

A Chief Risk Officer (or an equivalent function) should be established to provide a centralized focus on the broader spectrum of institutional risks, including strategic and operational risks, and

to ensure compliance considerations are integrated into enterprise risk management and decision-making processes.

## **2. Reinvigorate Governance Structures**

Reestablish formal oversight committees with defined charters, cadence, and system representation.

Lead Office: President's Office / EVPFO / OIC / Audit & Compliance Committee

Timeframe: Short-Term (6–12 mo.)

The University should reestablish the Executive Oversight Compliance Committee (EOCC) and the President's Policy Committee (PPC), or their equivalents, to restore clear governance, strengthen institutional accountability, and ensure that compliance and policy oversight are coordinated at the highest levels. Both committees should operate with defined charters, regular meeting schedules, and transparent reporting pathways to the President's Cabinet and the Board of Regents Audit and Compliance Committee.

The EOCC should focus on strategic oversight of compliance activities across the system, reviewing risk trends, assessing the effectiveness of compliance programs, and ensuring institutional priorities align with evolving regulatory requirements. Membership should include senior leaders from academic, administrative, and campus units to ensure representation of systemwide perspectives and needs.

The PPC should provide structured oversight of the University's policy development and review process. Including Chancellors and key system representatives would promote consistency and shared understanding across campuses. The PPC should also serve as an advisory body for evaluating the policy implications of compliance findings and emerging risks identified by the EOCC.

## **3. Strengthen Privacy & Data Security**

Develop a Privacy Office or designate a Chief Privacy Officer to unify FERPA, HIPAA, and similar (e.g., GDPR) compliance requirements and activities.

Lead Office: EVPFO / OIC / OGC

Timeframe: Short-Term (6–12 mo.)

Establish a University-wide Privacy Office or designate a Chief Privacy Officer (CPO) to oversee compliance with privacy and data security regulations, including FERPA, HIPAA, GDPR, and other applicable federal and state requirements. This leadership function should guide a unified privacy governance framework that defines principles, assigns decision-making authority, and coordinates IT, research, healthcare, and administrative units.

To enhance coherence and reduce fragmentation, the University should, where appropriate, align and integrate existing privacy and compliance functions under the Office of Institutional Compliance (OIC). This includes exploring the organizational realignment of the Health Information Privacy and Compliance Office (HIPCO) to strengthen coordination among privacy, data protection, and regulatory oversight activities.

#### **4. Administratively Align the Chief Auditor to the University of Minnesota Executive Structure**

To strengthen institutional oversight, improve coordination across audit, compliance, and risk functions, and enhance leadership accountability, the University should administratively align the Chief Auditor to the University's executive leadership structure while preserving the functional independence required for audit integrity.

Lead Office: Board of Regents / President

Timeframe: Long-Term (3-6 mo.)

The Board of Regents and University leadership should establish a dual-reporting model for the Chief Auditor that will improve visibility into systemic risks, ensure audit findings are appropriately escalated and addressed, and support stronger collaboration across institutional oversight functions without compromising audit independence.

- **Functional Reporting:** The Chief Auditor will continue to report functionally to the Board of Regents' Audit and Compliance Committee, preserving independence, objectivity, and direct governing authority oversight.
- **Administrative Reporting:** The Chief Auditor will report administratively to the Board of Regents Treasurer which, as defined by the *Bylaws of the Board of Regents*, is the Executive Vice President for Finance and Operations (EVPFO), enabling integration with executive leadership, enterprise risk management, and compliance coordination.

#### **5. Modernize Compliance Infrastructure & Tools**

Assess compliance infrastructure and tools, prioritize needs, and implement shared technology for training, reporting, and policy management.

Lead Office: OIC / OIT

Timeframe: Medium-Term (12–24 mo.)

Tools:

- Conduct a comprehensive assessment of compliance tools across the University to identify gaps, redundancies, and opportunities for greater alignment. Based on this assessment, prioritize technology needs and develop investment plans.
- To preserve flexibility and encourage innovation, the University should develop a catalog of pre-assessed, approved “plug-and-play” tools that meet University security and

compliance standards. Units could select from these approved solutions to meet specialized needs while maintaining systemwide consistency and oversight.

Data Access and Management:

- With units managing secure data on internal or external systems, implement a coordinated framework that ensures the protection, integrity, and timely access. The framework should include protocols for onboarding data systems, identifying and training assigned personnel, and creating a standardized process to support units in the timely execution of compliance and reporting functions.

## **6. Standardize Training & Onboarding**

Launch a role-based compliance curriculum and automate training assignments through onboarding/offboarding workflows.

Lead Office: OHR / OIC

Time Frame: Medium-Term (12–18 mo.)

To address these challenges, the University should develop a comprehensive compliance education framework that strengthens awareness, accountability, and accessibility across the system. This framework should

- Identify and assign compliance training by job type or position. Make information available through the automated training management system and/or other channels for compliance positions and their supervisors.
- Assess and provide recommendations to enhance the capability to deliver live, interactive training on new or updated compliance requirements and policies. The assessment should include establishing a capability for any compliance officer or unit to provide compliance content.
- Assess current capability for a centralized tracking and flagging system to monitor training completion and identify areas of non-compliance, ensuring timely follow-up and accountability.

## **7. Map & Clarify Compliance Roles**

Create a systemwide compliance role inventory to clarify ownership, reduce overlap, and align accountability.

Lead Office: OIC / Campus Compliance Offices

Timeframe: Short-Term (6–12 mo.)

Create a comprehensive, systemwide compliance role inventory to map all compliance-related responsibilities—both formal and functional—across academic, administrative, research, and operational units. The inventory should identify who holds primary, shared, and supporting roles

for each compliance area, as well as existing reporting lines and coordination points between campuses and central offices. Make information discoverable to all compliance officers and functions.

## **8. Establish a Centralized International Compliance Function**

Create a centralized function to provide leadership, oversight, and coordination for all international compliance activities.

Lead Office: OIC / Campus Compliance Offices

Timeframe: Short-Term (6–12 mo.)

Create a function to serve as the institutional hub for global regulatory compliance, ensuring that activities involving international research, data, partnerships, and imports/exports are managed consistently and in accordance with applicable laws and University policies. A variety of structural mechanisms can accomplish the function, including establishing an office, designating an international compliance position, or creating a network of existing positions assigned international compliance roles and responsibilities.

This central function should oversee and coordinate compliance in key areas, including data privacy (e.g., GDPR and other foreign privacy laws), research oversight and international collaborations, and import/export controls. It should develop standardized procedures for reviewing and approving international Memoranda of Understanding (MOUs) to ensure compliance with legal, privacy, and institutional risk requirements. A unified international policy framework should be created to guide faculty, staff, and administrators in navigating compliance obligations related to international research, contractual activities, and business operations. This framework should include a process for ongoing monitoring of evolving international regulations.

## **9. Improve Collaboration and Communication**

Recharter the Compliance Partners group with a clear purpose and objectives.

Lead Office: OIC

Timeframe: Short-Term (6–12 mo.)

The Compliance Partners group should be rechartered into a more active community of practice with refreshed purpose and objectives. This effort should review the original 2004 roles and responsibilities that outlined active strategic planning, assessment, monitoring, reporting, corrective action, and process improvement tasks. The group should serve as a systemwide forum for coordination, shared learning, and collective problem-solving across campuses and functional areas. The reestablished group should include representatives from key compliance domains and include system representation.

The group should function as a community of practice, rotating meeting leadership, highlighting emerging topics (such as AI ethics, NIL, or international compliance), creating peer groups (e.g., clinical healthcare delivery), and using data to monitor trends and address shared challenges.

## **10. Conduct Biennial Compliance Maturity Assessments**

Evaluate compliance performance, benchmark progress, and identify new improvement opportunities.

Lead Office: OIC / Internal Audit / External Reviewer

Timeframe: Long-Term (24–36 mo.)

The University should establish a process for conducting biennial compliance maturity assessments to evaluate the overall effectiveness and evolution of its compliance program. These assessments should measure progress against established benchmarks, assess the consistency and impact of compliance practices across campuses, and identify emerging risks or areas for improvement. The assessment process should encompass both quantitative and qualitative measures, including policy compliance rates, training completion data, audit findings, and stakeholder feedback.

## **Individual Recommendations from Interviewees**

The following recommendations were provided by those interviewed. In most instances, the recommendations listed were provided by multiple interviewees and have been summarized here. These recommendations have been thematically categorized.

### **Governance and Oversight**

- Expand the Compliance Partners group to include additional units and functions across the system, improving coordination and shared accountability.
- Increase the role of Internal Audit and the Compliance Committee to incorporate more compliance activity, oversight, and coordination with risk management.
- Add the Chancellors to the President’s Policy Committee (PPC) to ensure systemwide visibility and shared leadership in compliance and policy development.
- Reduce excessive decentralization to promote continuity, consistency, and clear lines of accountability.

- Consolidate operational compliance functions where feasible to strengthen efficiency and reduce duplication.
- Clarify the mission and portfolio of the Office of Institutional Compliance (OIC) to establish its authority, scope, and relationship with system partners.
- Reestablish and regularly convene the Compliance Partners group to share updates, review policy drafts, and align priorities.
- Designate a senior compliance leader (“leader I can consult with”) to serve as a trusted point of contact for escalation and decision-making.
- Place HIPCO (Health Information Privacy and Compliance Office) under OIC to unify oversight of privacy, security, and health-related compliance functions.
- Establish a central function to assess new laws and regulations and evaluate who is impacted, what actions are required, and what resources are needed for compliance.

## 2. Policy and Culture

- Implement University-wide responses to new policies to ensure consistent interpretation and application across all campuses.
- Develop a policy on emailing legislators from University accounts, clarifying that such communication reflects personal opinions, not institutional positions.
- Change the culture of reporting by encouraging open communication, normalizing escalation, and ensuring compliance information reaches the right audiences.
- Train the top 400 University leaders on audit and compliance processes, clarifying their roles in promoting compliance, monitoring risk, and supporting transparency.
- Create a Compliance Resource Directory (“Rolodex”) listing contacts, policies, activities, and subject-matter experts to improve access to compliance support.

## Education and Training

- Assign standard compliance training by job type to ensure a consistent baseline of understanding across all positions. Allow supervisors to adjust or waive assigned training when appropriate, provided they justify the decision and document the action.

- Expand live and interactive training opportunities and update online content regularly to maintain engagement and relevance.
- Provide compliance orientation for new faculty, supervisors, and staff that outlines reporting obligations and role-specific responsibilities.
- Develop peer networks and cohorts to enable compliance professionals to share best practices, discuss emerging issues, and collaborate on solutions.

### Technology, Data, and Systems Integration

- Adopt a unified IT system for compliance and reporting across campuses to reduce duplication and improve efficiency.
- Create a catalog of approved, pre-assessed “plug-and-play” IT solutions that can be easily implemented by units while ensuring security and compliance.
- Conduct pre-implementation assessments for University-wide IT systems to determine cost, feasibility, and resource implications.
- Develop a new UReports system to organize, manage, and monitor compliance reports more effectively.
- Implement oversight for IT and service purchases under \$50K to ensure small-scale acquisitions comply with privacy, security, and data standards.
- Encourage the IT procurement process to consider contracting compliance technology for University-wide uses (economies of scale) to reduce redundancy and ensure consistency across the system.
- Create a University-wide data privacy program encompassing FERPA, HIPAA, and other regulatory domains.
- Add or strengthen a Privacy and Security Office responsible for enterprise-level data governance, cybersecurity, and regulatory alignment.

## System Alignment and Collaboration

- Enhance system alignment for compliance by connecting positions with similar functions (e.g., Athletics, Veterans Affairs, Immigration) across campuses to collaborate and standardize practices.
- Share specialized personnel by function, for example, experts in VA benefits, international compliance, or export controls, to increase capacity and reduce redundancy.
- Encourage a network-based approach to compliance, ensuring that individuals in similar roles can consult and support one another across units.
- Share compliance trends, issues, and best practices through regular meetings, communications, or dashboards that track systemwide activity and emerging risks.

## Risk Management and Continuous Improvement

- Overhaul and modernize the compliance risk review process to identify gaps against the seven elements of an effective compliance program and establish action plans for follow-up.
- Use systems technology to map and monitor compliance risks across units.
- Conduct ongoing capacity and maturity assessments to evaluate readiness, alignment, and opportunities for improvement.
- Institutionalize accountability metrics and monitoring to track progress, ensure follow-through, and measure the impact of compliance initiatives.

# Framework for Strengthening Institutional Compliance

Board of Regents | Audit & Compliance Committee | April 9, 2026

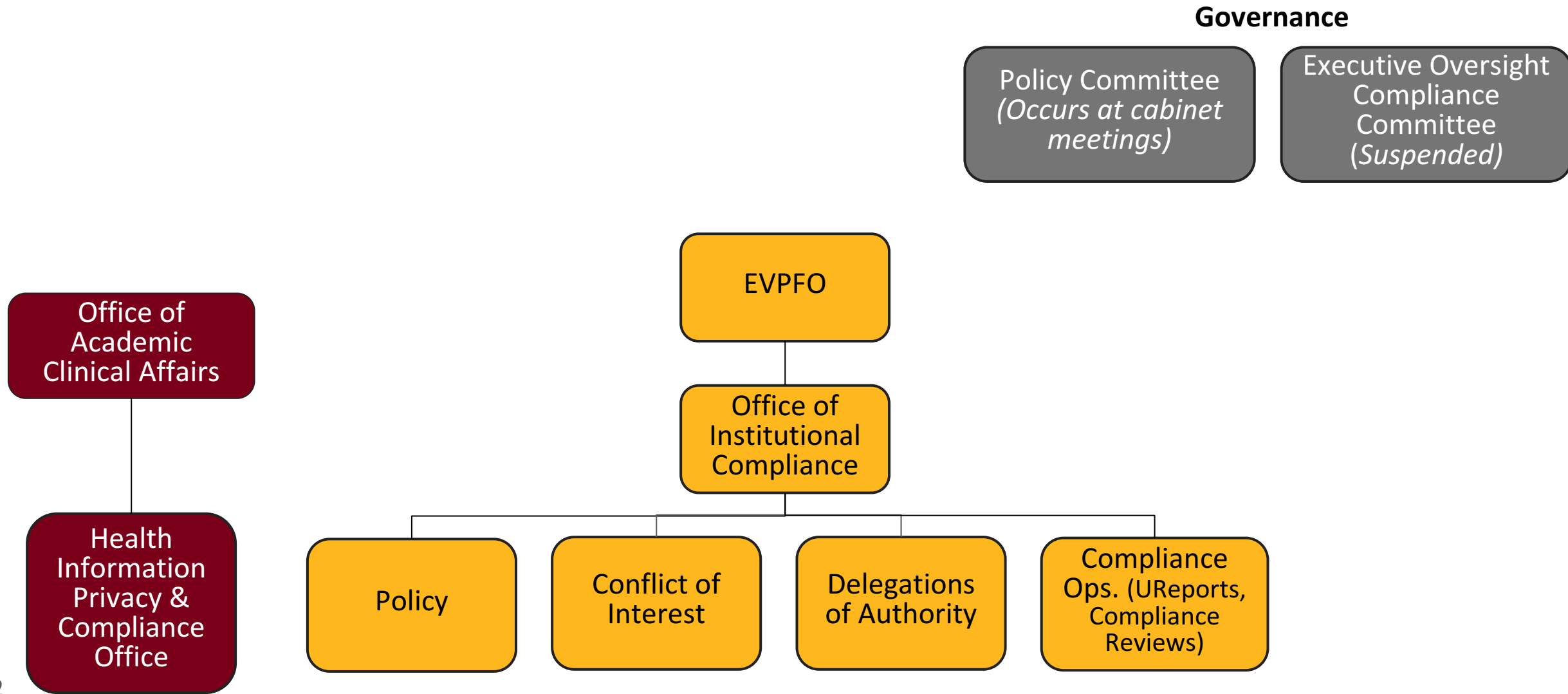
**Gregg Goldman**

Executive Vice President for Finance and Operations

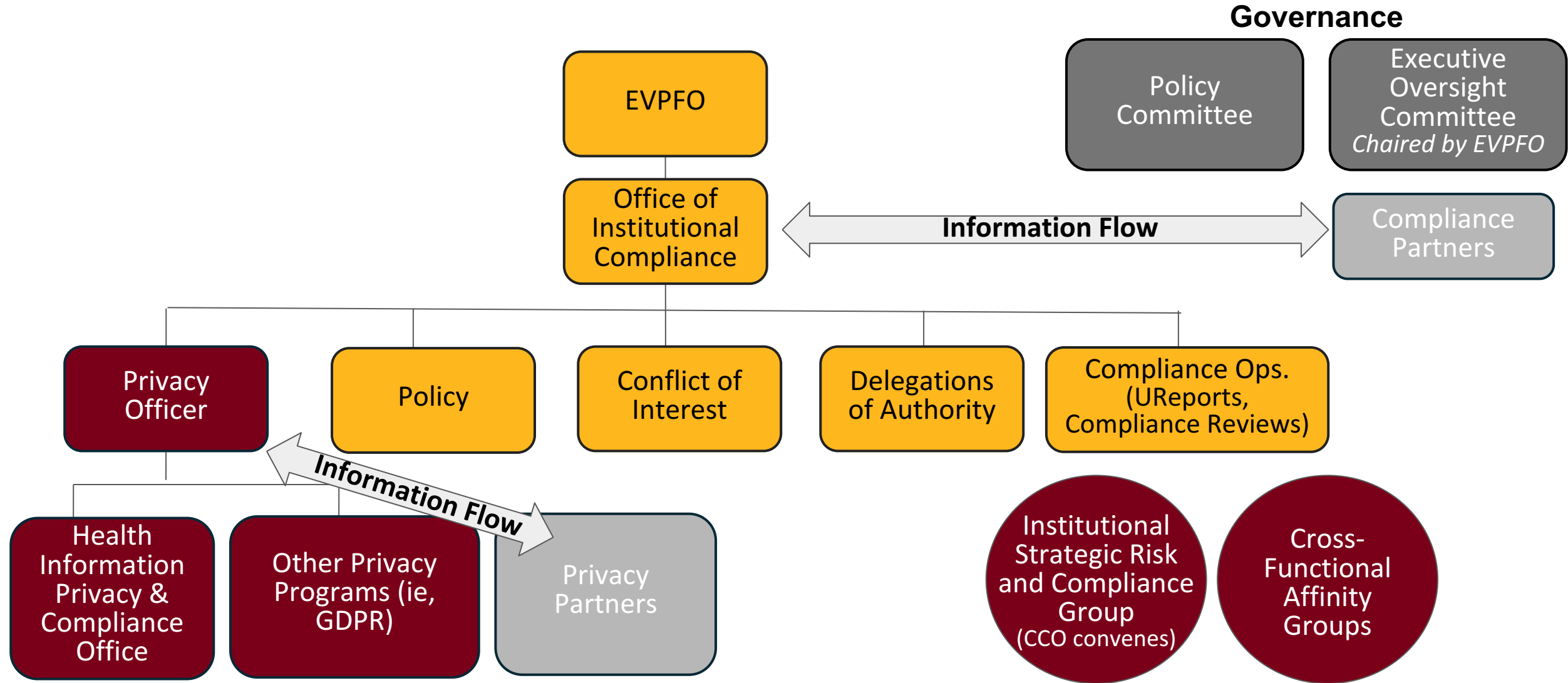


UNIVERSITY OF MINNESOTA

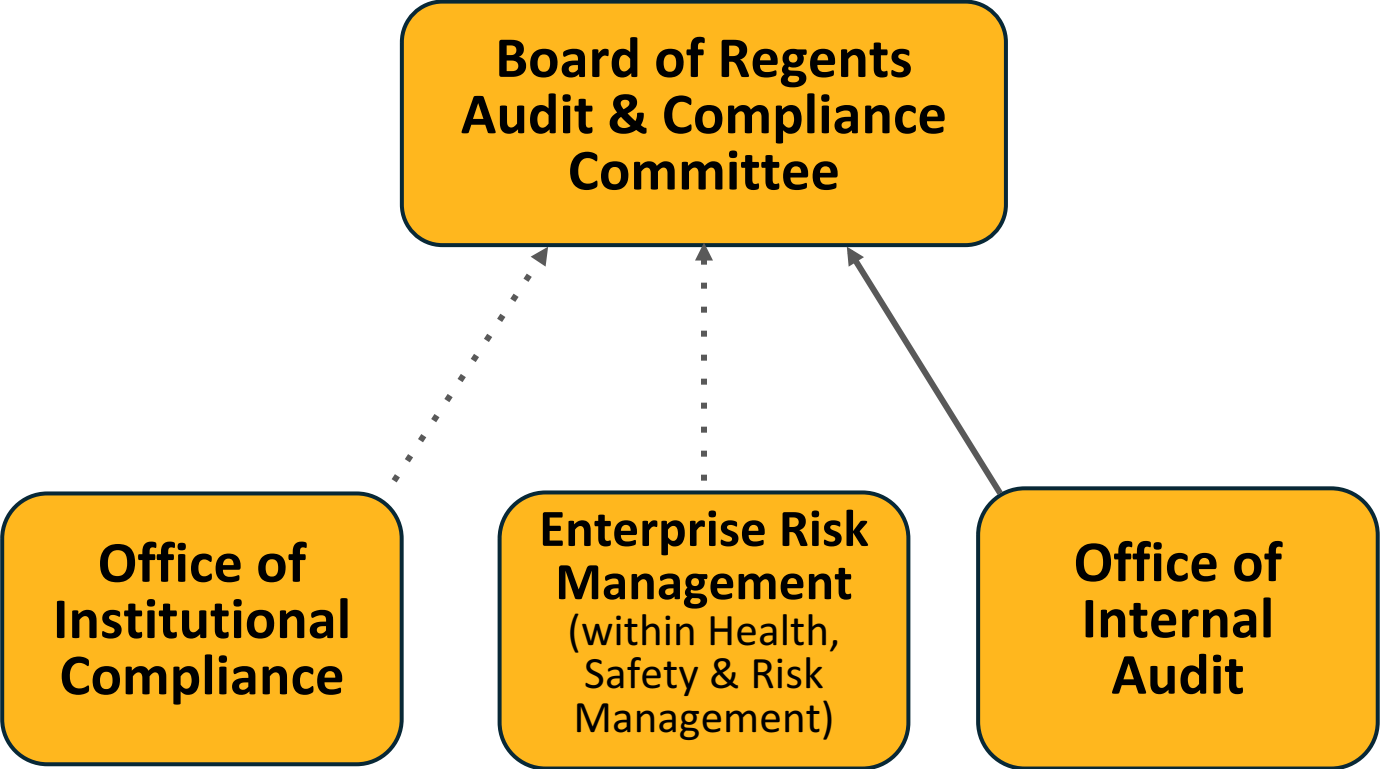
# Institutional Compliance - Current State



# Institutional Compliance - Future State



# No Change to Audit and Compliance Oversight Reporting



# Institutional Strategic Risk & Compliance Group

Institutional  
Strategic Risk and  
Compliance Group  
(CCO convenes)

## What

- Evaluate and assess **institutional** compliance risks and frameworks
- Coordinate cross-functional risk alignment and escalation
- Convened by the Chief Compliance Officer
- Inform EOCC, EVPFO and senior leadership
- Solicit, review and escalate compliance issues as identified by Compliance Partners and Affinity groups.

## Who

- Office of Institutional Compliance (Convenes)
- Enterprise Risk Management (in Health, Safety, and Risk Management)
- Information Security
- Office of General Counsel
- Internal Audit
- Research Compliance
- *Others could be added upon arrival of new Chief Compliance Officer and continuing discussions with leadership*

# Compliance Partners

## Compliance Partners

### What

- University-wide network of designated compliance professionals responsible for establishing and overseeing policies and processes to ensure compliance by function for the institution
- Structured like the RRC accountability model
- Dotted-line informational alignment to the Chief Compliance Officer
- A centralized forum for compliance communication, issue escalation, peer networking, and shared problem-solving to support consistent execution across units

### Who (examples)

Academic	Financial Aid
Accounting	Fundraising & Development
Accreditation	Governance/Policy
Admissions	Grants Management
Athletics	Hiring, Recruiting
Aux Services	Housing
Campus Safety/Clery	HR Operations (Leave, Payroll, etc)
Clinical Healthcare	Human Resources
Compensation	Immigration
Contracts & Procurement	Insurance
Copyright & Trademark	International Activities
Data Access and Privacy	IP & Tech Transfer
Disabilities	IT
Discrimination	Lobbying & Political
Employee and Labor Relations	Performance Management
Employee Benefits	Privacy & Info Security
Environmental Health & Safety	Program Integrity Rules
Equal Opportunity	Research
Ethics/Conflict of Interest	Retirement
Export Controls	Separation
	Sexual Misconduct
	Tax

# Cross-Functional Affinity Groups

Cross-  
Functional  
Affinity  
Groups

## What

- Organized around key risk and compliance areas (e.g., international, research, clinical care)
- Identify emerging compliance and risk issues
- Share information and best practices
- Engage with the Chief Compliance Officer
- Elevate significant issues to Institutional Strategic Risk and Compliance Group and the CCO

## Who (*Examples of Affinity Groups*)

- **International Compliance:** export controls, sanctions, travel risk, data privacy, international partnerships
- **Research Compliance:** research integrity, human and animal subjects, biosafety, export controls, sponsor requirements
- **Clinical Care Compliance:** HIPAA, clinical trials, patient and facility safety, billing requirements
- **Student Services Compliance:** student records and privacy (FERPA), conduct, accessibility, student wellbeing
- **Athletics Compliance:** NCAA, conference, student-athlete eligibility, health and safety, program integrity

# Reinvigorate Governance & Oversight

Policy  
Committee

Executive  
Oversight  
Committee  
*Chaired by EVPFO*

- Re-charter a systemwide executive compliance and risk oversight committee (similar to former EOCC)
- Reestablish the President's Policy Committee (PPC)
- Establish regular interaction between Office of Compliance to governance groups
- Implement dashboard reporting on trends, risks, and program maturity

# Next steps

1. Reestablish/reformat Policy Committee and Executive Oversight Committee
2. Hire Chief Compliance Officer; New CCO will evaluate opportunities from the compliance landscape analysis and recommend other program updates
3. Formalize:
  - a. Institutional Strategic Risk and Compliance Group
  - b. Compliance Partners
  - c. Cross-functional Affinity Groups
4. Hire Privacy Officer
5. Update Board of Regent Audit and Compliance Committee in December

# Discussion

- What cadence and types of updates would the Committee find most valuable (e.g., annual reporting, targeted updates, or topic-specific deep dives such as privacy)?
- What key indicators or measures would you expect to assess the effectiveness of the University's compliance program?
- What compliance and risk areas are most important for the Committee to focus on in the near term?
- How would the Committee like to receive information on emerging risks, compliance concerns, and institutional risk trends (including alignment with enterprise risk management)?

**Thank you!**



# BOARD OF REGENTS DOCKET ITEM SUMMARY

---

**Audit & Compliance**

**April 9, 2026**

**AGENDA ITEM:** Enterprise Risk Management and Institutional Risk Profile

**Review**

**Review + Action**

**Action**

**Discussion**

*This is a report required by Board policy.*

**PRESENTERS:** Katharine Bonneson, Associate Vice President, Health, Safety & Risk Management

## **PURPOSE & KEY POINTS**

The purpose of this item is to provide an update on the administrative governance supporting the Enterprise Risk Management (ERM) program, next steps for key deliverables including the Institutional Risk Profile, and an overview of expected changes in ERM work products.

Discussion will include:

- an updated ERM administrative governance framework;
- an overview of past and future processes for developing the Institutional Risk Profile; and
- review and discussion of new and updated ERM work products including risk reviews, and a risk scorecard.

## **BACKGROUND INFORMATION**

Creation of an ERM program was introduced to the Board during the 2021–22 academic year. Those committee meetings included initial ERM planning and discussion of attributes to include in a Request for Proposal (RFP) for an ERM consultant to support the program’s implementation. A contractor, Baker Tilly, was selected in fall 2022. An updated risk profile was created and previously presented to the committee at the September 2024 meeting with a broader discussion on the ERM program at the October 2025 meeting.

The Board previously discussed this topic at the following meetings:

- October 2025: *Enterprise Risk Management Program*, Audit & Compliance Committee
- September 2024: *Enterprise Risk Management (ERM) Program: 2024–25 Initiatives*, Audit & Compliance Committee
- May 2024: *Enterprise Risk Management (ERM) Program Update*, Audit & Compliance Committee
- September 2023: *Updates to the Institutional Risk Profile*, Audit & Compliance Committee

- May 2023: *Progress Report on the University's Institutional Risk Profile*, Audit & Compliance Committee
- February 2023: *Enterprise Risk Management (ERM) Program Update*, Audit & Compliance Committee
- May 2022: *Enterprise Risk Management Update and Discussion*, Audit & Compliance Committee
- December 2021: *MPact 2025 Update: Enterprise Risk Management Plan*, Finance & Operations Committee

# Enterprise Risk Management Update and Institutional Risk Profile, April 2026



ENTERPRISE  
RISK MANAGEMENT

UNIVERSITY OF MINNESOTA

**Driven to Discover®**



HEALTH, SAFETY,  
AND RISK MANAGEMENT

UNIVERSITY OF MINNESOTA

# Agenda

1. Introduction
2. Governance Update
3. Risk Profile & Risk Products
4. Work Plan and Lessons Learned



# Introduction, ERM Trends

**Political and Economic uncertainty are top of mind, AI is viewed as a significant emerging risk and opportunity.**

**Across Higher Ed., risk managers are experimenting with dashboards, profiles and products that provide flexible, actionable guidance to support leader decision making.**

**Data Security & Cybersecurity along with enrollment remain consistent as top 5 risks over the last 4 years.**

**Clear governance and support from senior leaders are viewed as key ingredients for ERM impact and success.**



# UMN's ERM Program

- Enterprise Risk Management (ERM) was established in spring, 2022 as a method to proactively manage risk and opportunities strategically across the system. The program is housed in Health, Safety & Risk Management and supported by a full time manager.
- Initial program deliverables included
  - Inaugural Risk Profile (2023)
  - Updated Risk Profile (2024)
  - Risk Deep Dives (2023 - 2025)
  - Ad hoc unit-level assessments
- In 2025, the ERM group paused the Risk Profile and Deep Dive process to align with governance and oversight updates in the Compliance/Risk landscape.



# ERM Governance Update

- Building off of the Compliance Landscape project led by the EVP for Finance and Operations, the goal for ERM is to reinvigorate governance and oversight to support major initiatives such as the risk profile, risk assessments and scorecard development.
- The Executive Oversight Committee (EOC) will provide guidance and oversight to the ERM program with additional review and approval from the President's Cabinet.
- This governance structure supports strong collaboration between the Office of Institutional Compliance and ERM, as both teams will work through the EOC.



# Institutional Strategic Risk & Compliance Group

- Engagement of the Institutional Strategic Risk & Compliance Group will be instrumental to advancing ERM initiatives.
- ***\*Referenced in the Compliance Landscape presentation,*** members include; OIC, ERM, Privacy, Information Security, OGC and OIA.
- This flexible working group provides an opportunity to elevate and coordinate discussions on;
  - Risk opportunities
  - Emerging risks
  - Insights on the impacts of decision making
  - Trends and risk analysis
  - Risk profile



# Previous Risk Profile

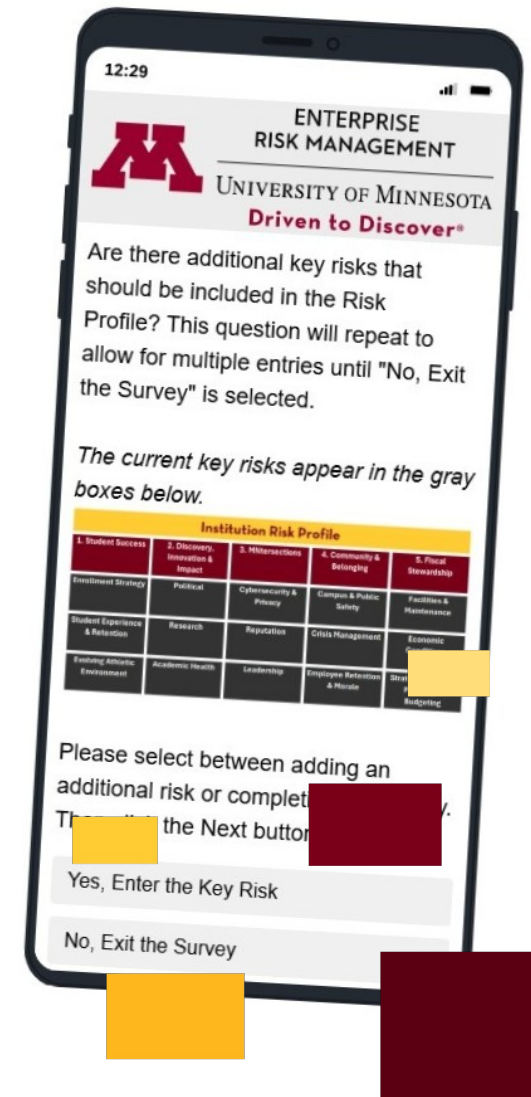
- Sept. 2023: the first Institution Risk Profile was presented to Audit & Compliance Committee with the help of Baker Tilly
- Sept. 2024: Updated Risk Profile was presented to the Audit & Compliance Committee
- 2025: ERM group paused the Risk Profile process to align with governance and oversight updates in the Compliance/Risk landscape

Institution Risk Profile				
1. Student Success	2. Discovery, Innovation & Impact	3. MNtersections	4. Community & Belonging	5. Fiscal Stewardship
Enrollment Strategy	Public Policy & Government	Cybersecurity & Privacy	Campus & Public Safety	Facilities & Maintenance
Student Experience & Retention	Research	Reputation	Crisis Management	Economic Conditions
Evolving Athletic Environment	Academic Health	Leadership	Employee Retention & Morale	Strategic Financial Planning & Budgeting



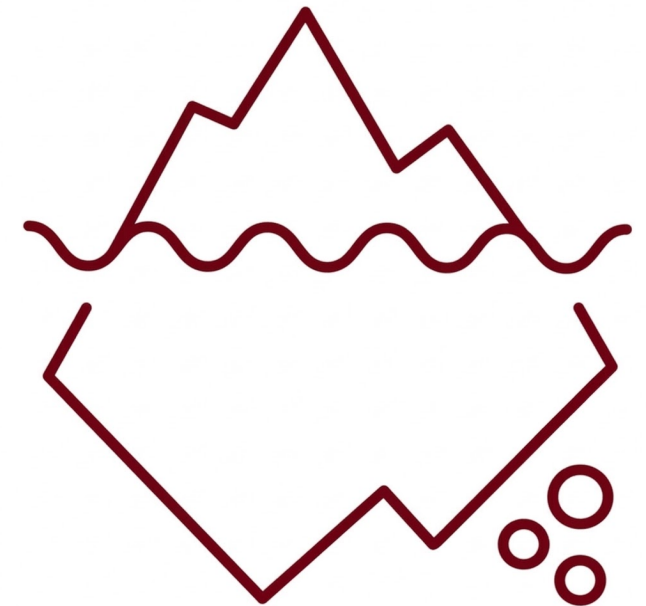
# Recommended Risk Profile Process

- Continue to use annual survey data from University leaders, adding representation from front-line staff and faculty (*change in process*), to inform the risk profile. Survey administration is planned to take place each spring.
- Upon gathering the survey results, work through the Institutional Strategic Risk and Compliance Group and the EOC/Cabinet (*change in process*) to verify and revise risk ranking and identification information. Review results against peer and industry benchmarks.
- Provide an updated profile for the Audit & Compliance Committee each fall, highlighting commonalities of risks, interrelated and emerging risks.




# Digging Deeper Into Risks

- Use the updated governance structure to elevate risk trends, concerns or opportunities and prioritize risks requiring a deeper analysis and review. Key principles for risk review success are:
  - Evaluating effectiveness of control and mitigation efforts
  - Assigning and engaging risk owners
  - Establishing repeatable, predictable review cycles
  - Connecting risks to strategic plan priorities
- This is not a one and done process. The goal is to track risks over time using a scorecard that monitors the progress of risk mitigation strategies.

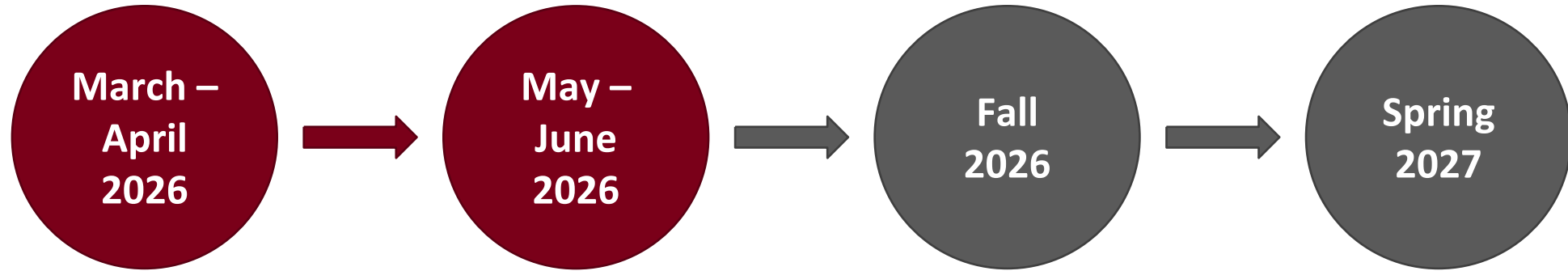


# Risk Scorecard Preview

- Scorecard Development: The purpose is to provide a mechanism that monitors and tracks trends of identified institutional profile risks.
- Scorecard aimed at supporting strategic discussions on risk trends and opportunities, with alignment to ***Elevate Extraordinary 2030.***

<b>Cybersecurity &amp; Privacy</b> Risk Owner: Chief Information Security Officer	 <b>High Risk</b>
<b>Risk Context</b>	<b>Management's Risk View</b>
<i>Example only - Not UMN information</i> The University is a steward of many types of private data from student and employee personal information to health related information for research participants and clinic patients. The University holds valuable intellectual property that could be the target of state-sponsored actors. The University is subject to various regulations including HIPAA, FERPA, and MGDPA.	<i>Example only - Not UMN information</i> <ul style="list-style-type: none"> <li>• Compliance is the baseline, not the goal; the University goes above and beyond regulatory requirements</li> <li>• The University keeps private data completely secure while not burdening researchers in their quest for new knowledge</li> <li>• There is good coordination across academic and administrative units to ensure security</li> </ul>
<b>Key Risk Drivers (Events that Change Risk)</b>	<b>Key Mitigating Actions</b>
<i>Example only - Not UMN information</i> <ul style="list-style-type: none"> <li>• A significant incident that have resulted in the theft and exposure of private data</li> <li>• Privacy regulations are becoming more stringent and the cost of failure is becoming higher</li> <li>• Emerging technologies like artificial intelligence are being used to launch more sophisticated cyber attacks</li> <li>• There is a very large and often transient database user group</li> </ul>	<i>Example only - Not UMN information</i> <ul style="list-style-type: none"> <li>• Administrative Policy: Data Security and Classification</li> <li>• IT system review and approval processes are in place</li> <li>• Technical controls and infrastructure such as multi-factor authentication, firewalls, and intrusion detection and monitoring tools</li> <li>• Required information security gap analysis performed by University colleges, departments, centers and so on)</li> </ul>
<b>Key Risk Indicators/Metrics</b>	<b>Emerging Issues/Comments</b>
<i>Example only - Not UMN information</i> <ul style="list-style-type: none"> <li>• Phishing click-through rate</li> <li>• Mean time to remediate (MTTR) vulnerabilities</li> <li>• Security gap analysis completion rate</li> <li>• Zombie account rate</li> <li>• Legacy system retirement rate</li> </ul>	<i>Example only - Not UMN information</i> <ul style="list-style-type: none"> <li>• Minnesota Privacy Act; this new privacy legislation (2025) has expanded the rights of consumers regarding their data.</li> <li>• Quantum Security; The Minnesota Technology Advisory Council has urged state entities to prepare for quantum-resistant encryption as this technology could leave current security measures vulnerable.</li> </ul>

# Work Plan, 2026 - 2027



## **Review Profile Process**

EVP team review, Cabinet review, Audit & Compliance Committee (ACC) Presentation

## **Implement updated profile process**

Launch survey and complete draft profile by July

## **Develop and implement risk review plans and dashboard**

Present the risk profile to the ACC

## **Proceed with annual risk profile refresh**

Supports cycle of presenting material in a regular cadence to the ACC (fall, 2027)

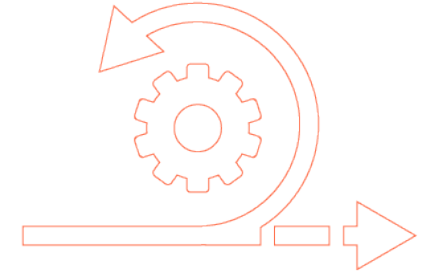


# Lessons Learned, 3 year Review

- ERM can be highly effective and is becoming the standard in higher education as a cornerstone of a risk management program.
- The governance structure is vitally important to hosting meaningful conversations, engaging leaders and developing impactful products.
- The risk assessment process must be nimble and efficient. Previous efforts to deep dive into risks were thorough, but challenging to produce with translatable findings.
- The ERM program will benefit from rechartering a standard package of deliverables on an agreed upon, repeating timeline.
- The **UMN's ERM program** is well positioned with reporting alignment in the EVP for Finance & Operations Office.



# Looking for Feedback



1. What are some ways that the Committee might use the Institutional Risk Profile to support broader strategic discussions in support of the University?
2. Are there emerging risks that you would like ERM to perform additional analysis on?



UNIVERSITY  
OF MINNESOTA  
Driven to Discover®

# Thank you!

Please feel free to reach out with additional questions.





# BOARD OF REGENTS DOCKET ITEM SUMMARY

**Audit & Compliance**

**April 9, 2026**

**AGENDA ITEM:** Information Items

**Review**

**Review + Action**

**Action**

**Discussion**

*This is a report required by Board policy.*

**PRESENTERS:** Quinn Gaalswyk, Chief Auditor

## **PURPOSE & KEY POINTS**

- A. Engagements with the University’s Appointed Independent External Auditor Requiring After-the-Fact Reporting
- B. Review of External Auditor Relationship and Services Provided

### **A. Engagements with the University’s Appointed Independent External Auditor Requiring After-the-Fact Reporting**

The purpose of this item is to report engagements with the University’s appointed independent external auditor, as required by Board policy.

- CliftonLarsonAllen LLP, the University’s appointed independent external auditor, was engaged to perform an agreed-upon procedure for certain University of Minnesota retirement plans for the year ended December 31, 2024. This engagement did not present an independence issue with CliftonLarsonAllen LLP. The fees for this engagement are estimated at \$32,000.

### **B. Review of External Auditor Relationship and Services Provided**

The purpose of this item is to review audit and non-audit services provided to the University by external audit firms and the related fees paid for those services related to FY 2025.

#### *External Auditor Review (Section I)*

CliftonLarsonAllen LLP (CLA) contracted audit and non-audit fees were \$667,650 for FY 2025 engagements, with actual fees of \$653,652 paid to CLA. All FY 2025 engagements have been completed. The fees represent what was billed for engagements. A summary of management’s evaluation of CLA’s performance for FY 2025 engagement is included in the docket.

#### *Summary of Audit and Non-Audit Services and Fees (Section II)*

Total fees of \$775,683 have been paid for FY 2025 engagements to CLA and two other public accounting firms for a variety of audit and non-audit services. A description of the services is included in the docket. All audit and non-audit services were reviewed by the Controller's Office for audit independence and approved by or reported to the Audit & Compliance Committee as required by Board of Regents Policy: *Board Operations and Agenda Guidelines*.

## **BACKGROUND INFORMATION**

Engagements with the University's appointed independent external auditor that do not impair independence are reported after the fact to the committee as required by Board of Regents Policy: *Board Operations and Agenda Guidelines*, Section IV, Subd. 6 (a).

The review of external auditor relationship and services provided report is prepared and presented to the Audit & Compliance Committee in conformity with Board of Regents Policy: *Board Operations and Agenda Guidelines*, Section IV, Subd. 6.

**UNIVERSITY OF MINNESOTA  
BOARD OF REGENTS AUDIT & COMPLIANCE COMMITTEE  
April 9, 2026**

**External Auditor Review and Summary of  
External Auditor Relationships and Services Provided**

**Background**

The Audit & Compliance Committee (AUD) is responsible for reviewing and evaluating the appointed independent external auditor's performance, independence, and effectiveness. Effective governance practice recommends that the AUD of the Board should conduct such a review at least annually. The AUD conducted its last review of audit services and fees in May of 2025.

The Controller's Office presents the information below and on the accompanying schedules for the AUD's review of audit, audit related, and non-audit services fees paid to external audit firms including CliftonLarsonAllen, LLP (CLA), the University's appointed independent external auditor through FY 2025 engagements. Also included is management's assessment of CLA's performance for the FY 2025 engagements.

**Section I - Annual Review of External Auditor Relationship and Performance**

University management and the CLA engagement management team met in January of 2026 and reviewed CLA's services and performance during the FY 2025 audit. University management also met with the CLA engagement management team regularly to discuss the progress of engagements. The overall conclusion was CLA provided excellent service for the FY 2025 engagements.

Relative to the strengths of CLA and the positive aspects of the engagements:

- The CLA team has significant higher education industry experience and continues to share ideas for potential future improvements;
- CLA's audit approach was both robust and fair, with regular and open dialogue with management supporting effective execution of engagements;
- Annual engagement fees have aligned with the contract and budget amounts.

Both the University and CLA have identified future opportunities for improvement and have begun implementing those improvements for the FY 2026 engagements. Areas of future improvement opportunities include:

- Suggestions for areas that can be tested earlier in the audit process, alleviating potential strains on resources;
- Continuing to enhance communications between both teams to ensure consistency and timeliness.

## **Review of Fees Paid to CLA**

The accompanying schedule presents a summary of fees paid to CLA for the various FY 2025 audits and other services. The top portion of the fee schedule represents fees paid for the University's annual institutional audits and audit-related engagements. The contract amounts reported on the schedule are consistent with the amounts agreed to in the FY 2025 engagement letters and the firm's fixed price contract for FY 2025. The total audit fees paid to CLA for FY 2025 were equal to the contract amounts in total. These amounts are final.

The lower portion of the schedule contains a breakdown of fees paid to CLA for other services. During the year, CLA performed one other engagement for a specific unit of the University. To reduce audit costs and maintain greater oversight of audit and audit-related engagements across the University, the Controller's Office worked closely with CLA and University departments to use CLA whenever possible for additional external audit or attest services during their appointment as the University's appointed independent external auditor.

Services performed by CLA during FY 2025 that were not part of the annual audits and NCAA agreed-upon-procedures of the University included:

- An agreed-upon-procedures engagement for certain University of Minnesota retirement plans for the years ended December 31, 2023 and 2022.

**UNIVERSITY OF MINNESOTA  
BOARD OF REGENTS AUDIT & COMPLIANCE COMMITTEE**

April 9, 2026

**Schedule I - Fees Paid to CliftonLarsonAllen, LLP  
FY 2025 Engagements**

<u><i>Annual Institutional Audit and AUP Engagements</i></u>	<i>FY 2025 Engagements</i>			<i>Total FY 2024</i>
	<i>Contract Amount</i>	<i>Billed Amount</i>	<i>Over/(Under) Budget</i>	<i>Prior Year Billed Amount</i>
University Financial Statement Audit	\$ 438,520	\$ 438,520		\$ 425,750
Compliance Audit (Federal 2-CFR 200 Subpart F & MOHE)	154,500	154,500		150,000
NCAA Agreed-Upon-Procedures – Twin Cities	21,630	21,630		20,875
NCAA Agreed-Upon-Procedures – Duluth				17,843
<b>Total Fees for Institutional Engagements</b>	<b><u>\$ 614,650</u></b>	<b><u>\$ 614,650</u></b>	<b><u>\$ 0</u></b>	<b><u>\$ 614,468</u></b>
 <u><i>Other Audit, Audit Related, and Non-audit Fees</i></u>				
Retirement Plan Agreed-Upon-Procedures	\$ 53,000	\$ 39,002	\$ (13,998)	
SOC2 Compliance Agreed-Upon-Procedures				\$ 33,600
Regenerative Medicine Agreed-Upon-Procedures				26,250
Medicare Cost Review				9,450
<b>Total Other Audit, Audit Related, and Non-Audit Fees</b>	<b><u>\$ 53,000</u></b>	<b><u>\$ 39,002</u></b>	<b><u>\$ (13,998)</u></b>	<b><u>\$ 69,300</u></b>
<b>Total Fees</b>	<b><u>\$ 667,650</u></b>	<b><u>\$ 653,652</u></b>	<b><u>\$ (13,998)</u></b>	<b><u>\$ 683,768</u></b>

## **Section II - Review of Fees Paid to All Other Auditing Firms**

In addition to the audits performed by CLA (the University's independent external auditors), other accounting and auditing firms performed a variety of audit and non-audit services at the University during FY 2025. These services were:

- Baker Tilly Virchow Krause & Co LLP was engaged by the Office of Vice President of Finance and Operations to develop a more robust Enterprise Risk Management (ERM) strategy and organizational structure to support risk management across the University of Minnesota.
- Baker Tilly Virchow Krause & Co LLP was engaged to complete the annual audit of the statutory financial statements for RUMINCO.
- Ernst & Young, LLP was engaged by the Tax Management Office to assist with tax filings in China and contract registration with Chinese Authorities.

The Controller's Office reviewed all of the contracts detailed on the attached schedule, consistent with Board policy. None of these engagements resulted in an impairment of independence, in fact or in appearance, for any of the firms.

**UNIVERSITY OF MINNESOTA  
BOARD OF REGENTS AUDIT & COMPLIANCE COMMITTEE  
APRIL 9, 2026**

**Schedule II - Report of Fees Paid to Audit Firms for FY 2025 Engagements**

<u><i>Audit Firm</i></u>	<u><i>FY 2025 Engagements</i></u>			<u><i>FY 2024</i></u>
	<u><i>Audit Fees</i></u>	<u><i>Non-Audit Fees</i></u>	<u><i>Total Fees</i></u>	<u><i>Total Fees</i></u>
Baker Tilly Virchow Krause & Co, LLP	\$ 29,290	\$ 19,771	\$ 49,061	\$ 88,072
CliftonLarsonAllen, LLP	614,650	39,002	653,652	683,768
Deloitte & Touche, LLP				26,500
Ernst & Young, LLP		72,970	72,970	18,390
Moore Stephens & Butterfield				24,500
<b>Total Fees Paid</b>	<b>\$ 643,940</b>	<b>\$ 131,743</b>	<b>\$ 775,683</b>	<b>\$ 841,230</b>