Audit & Compliance Committee

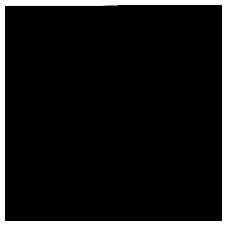
May 2024

May 9, 2024

8:00 AM

Boardroom, McNamara Alumni Center

3

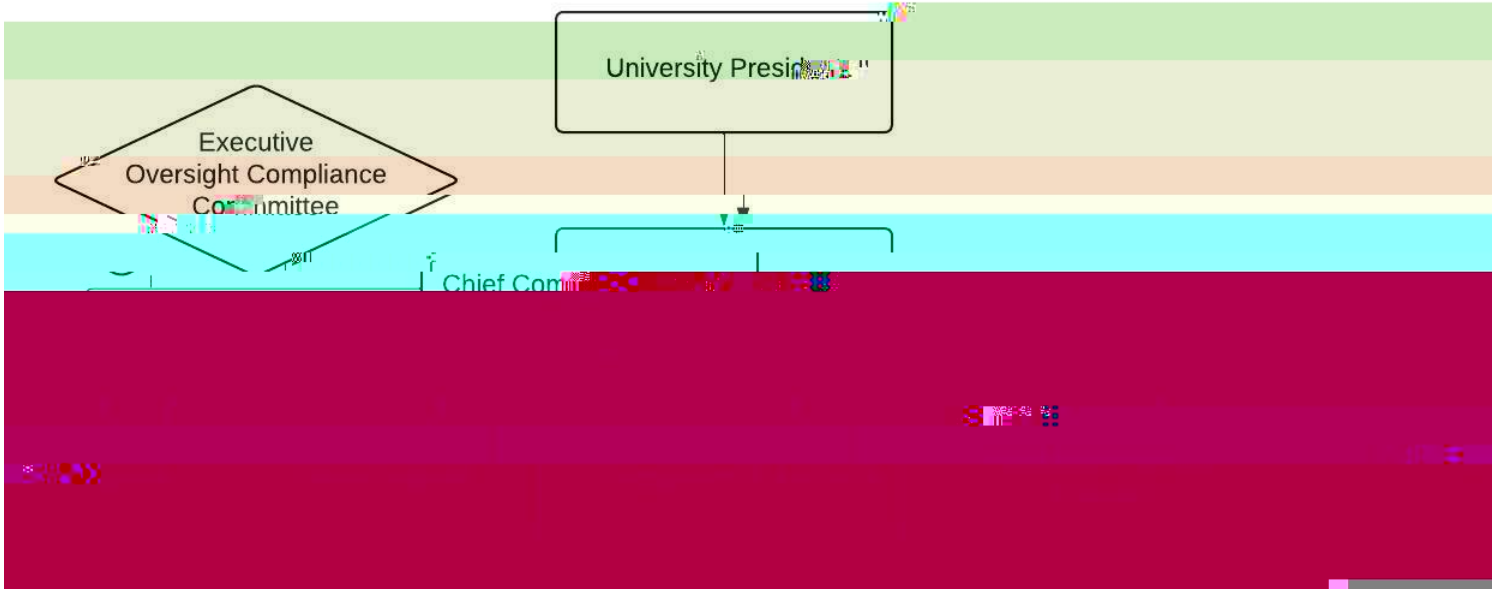



UNIVERSITY OF MINNESOTA

Office of Institutional Compliance (OIC)

- OIC consists of four programs that report to the University's Chief Compliance Officer:
  - Compliance Program
  -

OIC Structure



Compliance Program

- Established in 2006 and follows the elements of the Federal Sentencing Guidelines
- The program manages approximately 250 hotline reports each year, annually conducts 2-3 in-depth compliance area risk reviews, and convenes triannual meetings of the Executive Oversight Compliance Committee and Compliance Partner Committee

Data Privacy vs. Security

- Privacy: the right to have control over how your personal information and data are collected, stored, and used

- Security: the protection of personal information and data from potential breaches and leaks

Data Privacy vs. Security

- University Information Security, a division of OIT, has responsibility for data security policies, oversight and some key controls.
- Strictly looking at data privacy in this presentation
- Key privacy aspects:
  - What types of data should be collected?
  - Who has access to the data once collected?
  - How can someone limit or request deletion of their data once collected?

Privacy Management - HIPAA

- Applies to UMN units in the Health Care component or those supporting these units
- Privacy responsibility held by Health Information Privacy and Compliance Office (HIPCO) within the Medical School's Office of Academic Clinical Affairs
- Key privacy requirements include:
  - All employees/students that handle protected health information required to take HIPAA training
  - Business Associate Agreements (BAAs) established with external parties with access to HIPAA data

Privacy Management - FERPA

- Provides students rights around accessing, amending, and disclosure of their educational records
- Primarily overseen by Academic Support Resources under the Provost’s Office
- Key privacy requirements include:
  - Academic Support Resources employees and all others that access student records must take required training

Privacy Management – PCI DSS

- Departments that accept payment cards as payment for goods and services are contractually obligated to follow
- Primarily overseen by the Payment Card Compliance Office in the Controller's Office
- Key privacy responsibilities include:
  - Training program for all employees who have access to a customer's cardholder data
  - Periodically confirming and reporting on compliance

Privacy Management – Other Regs

- Minnesota Government Data Practices Act regul ±
  - Data requests by the public handled by the Data Accpic handled by

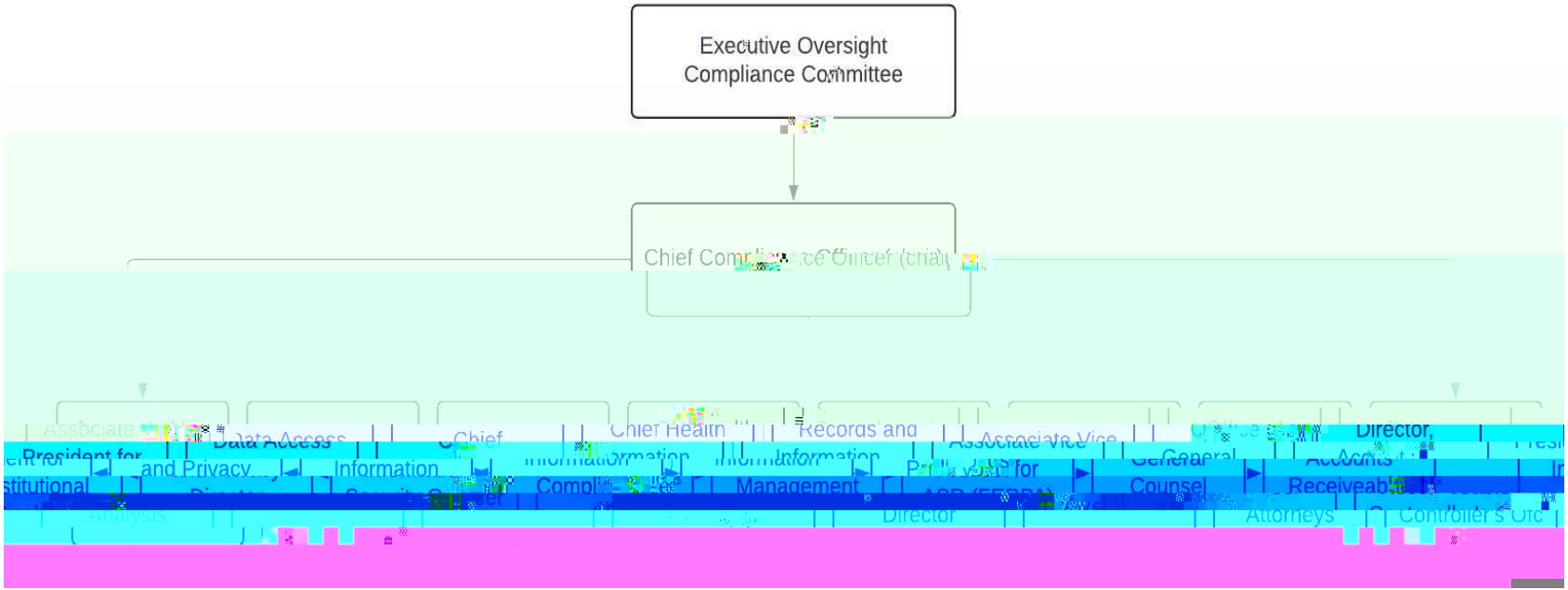
PCIS Committee Charge

- The Privacy, Confidentiality, and Information Security (PCIS)
  - Charge is to monitor major developments to privacy, confidentiality and security on behalf of the Executive Oversight Compliance Committee, and identify issues and opportunities for improvement
  - Meets as needed including 3 times in FY24

Privacy Management – PCIS Committee

- PCIS Committee was tasked at the July 2023 Executive Oversight Compliance Committee meeting:
  - Strengthening oversight and coordination of data privacy functions
  - Identify, evaluate and escalate data privacy concerns identified by units' outside of regular responsibilities or current established review processes

PCIS Committee Membership



PCIS Committee Initiatives

- Established “guiding principles” for privacy to inform University and unit business decisions that may impact individuals’ privacy
  - Principles include: Privacy by design; transparency and notice; choice; information review and correction; information protection; and accountability

PCIS Committee Initiatives

- Creating a tracking tool where committee members can report privacy questions that they are fielding to get a sense of scope

- Taking an early look at the creation of a University-wide privacy policy to address privacy issues

[redacted]

Enterprise Risk Management (ERM) Program Update

☐ ☐ ☐ ☐

Katharine Bonneson, Associate Vice President, Health, Safety & Risk Management
Matt Reierson, Senior Manager, Baker Tilly

The purpose of this item is to provide the committee with an update on the University's Enterprise Risk Management (ERM) Program. Part of the discussion will outline the initial risk assessment of three top risks that were highlighted to the committee at the September 2023 meeting. The establishment of an ERM program, a component of the MPact 2025 Systemwide Strategic Plan, is underway.

A di & Compliance Commi ee
Ma 2024

ERM work plan review

Risk analysis process

Overview of crisis response, facilities and leadership

Broad risk overview, emerging risks

Next steps

ERM p n was launched in 202 thod to as sk
holisti University's
goals
Baker help establish the Institution
Profile, which was presented to the Committee in September, 2023
The program lives within Health, Safety & Risk Managem 2024G 1/6 ives w2

Objective of risk analysis - identify and prioritize sub-risks that could impact achievement of our strategic goals

- Gather data, internally and externally (peer institutions). Review past events, MSU, AZ, UMN events
- Facilitate individual discussions with Subject Matter Experts
- Review existing risk related reports (Facility Condition Report for example)

Key Questions:

What could go wrong and how likely is it to occur?
How do we compare to our peers?
Which risks are the highest priority?
What would this look like in 3 to 5 years?

Strength, in all categories, our employees ability to adapt and dedication to the University reduces risk, keeps the University working

Risk, decentralized nature allows for variable levels of consistency and adoption of guidelines and standards

Observation, the University is a map of ‘have and have nots’ with some schools and colleges in a much better position to reduce risk exposure than others

High enthusiasm for hosting conversations about risk across units and all campuses

(Defined as,

Analysis included: interviews, review of policies/procedures, event and incident reviews, after-action reports

Risk Summary
Medium risk. Plans and crisis response frameworks are in place however the effectiveness, communication and increased velocity of events equates to a higher inherent risk.

Overall Observations

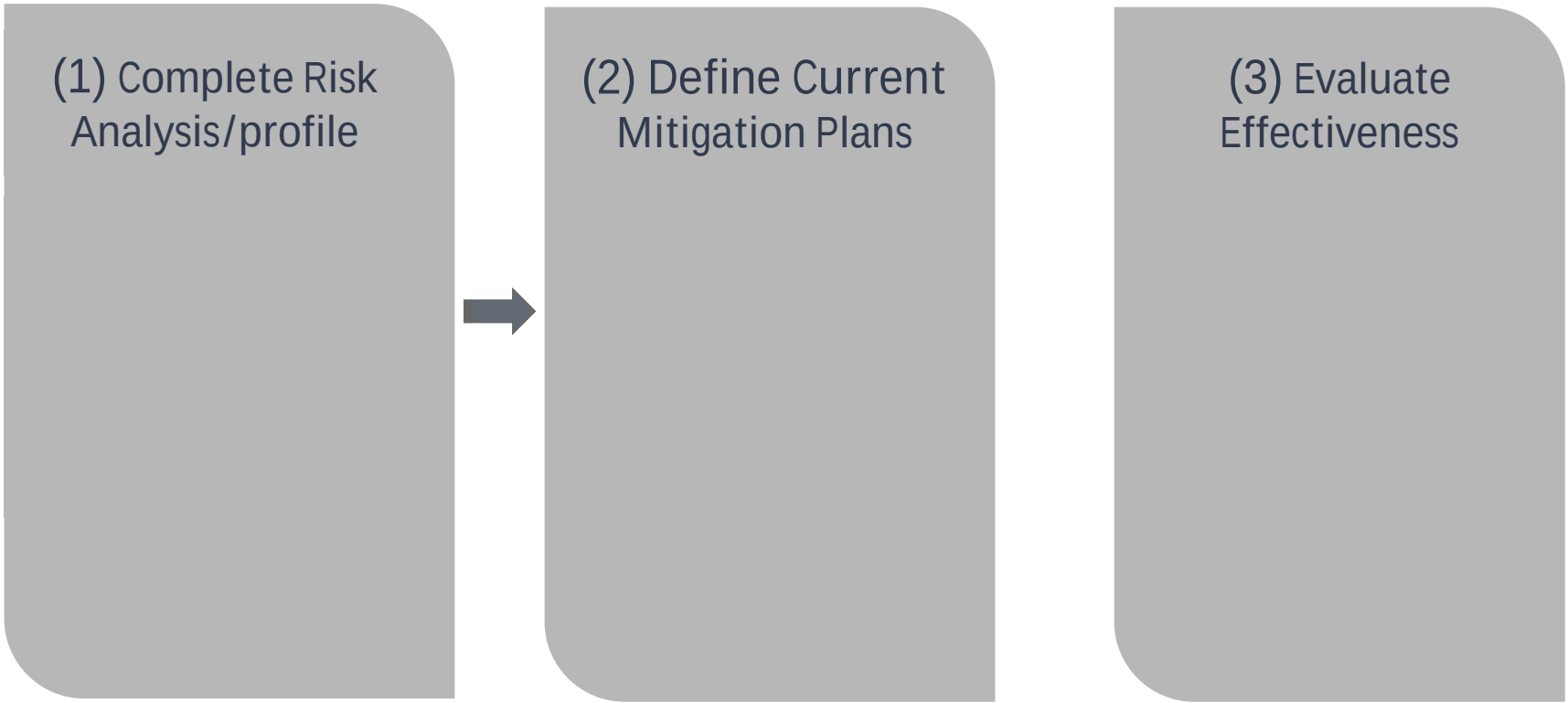
- Lack of awareness of plans & processes
- Communication challenges, siloed behavior
- High community expectations
- Unpredictability of social media influence

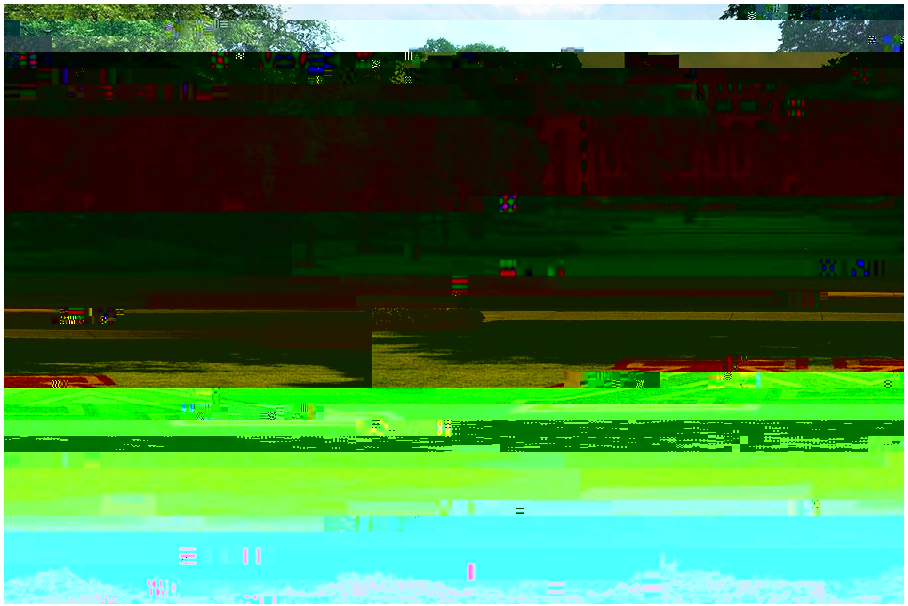
Areas of Strength

- Staff are experienced and capable
- Appropriate continuity and emergency plans and response frameworks exist
- COVID provided excellent training opportunities

Risks

- Unified command is not always supported (decentralized nature)
- Communication can be siloed
- Plans may not be effective due to lack of awareness or practice
- Leadership transitions lead to gaps in knowledge and decision-making
- Notification and data sharing expectations from the [illegible] frustration


(1) Complete Risk Analysis/profile
(2) Define Current Mitigation Plans
(3) Evaluate Effectiveness



BOARD OF REGENTS

DOCKET ITEM SUMMARY

Audit & Compliance May 9, 2024

AGENDA ITEM: Information Items

☐ Review	☐ Review + Action	☐ Action	☒ Discussion

PRESENTERS: Quinn Gaalswyk, Chief Auditor

PURPOSE & KEY POINTS

The purpose of this item is to report audit and non-audit services provided to the University by external audit firms and the related fees paid for those services related to FY 2023.

External Auditor Review (Section I)

UNIVERSITY OF MINNESOTA

UNIVERSITY OF MINNESOTA
BOARD OF REGENTS AUDIT & COMPLIANCE COMMITTEE
May 9, 2024
Schedule I - Fees Paid to Deloitte & Touche, LLP
FY 2023 Engagements

	FY 2023 Engagements	*Total FY 2022*
Annual Institutional		

Section II -

UNIVERSITY OF MINNESOTA
BOARD OF REGENTS AUDIT & COMPLIANCE COMMITTEE
MAY 9, 2024

Schedule II - Report of Fees Paid to Audit Firms for FY 2023 Engagements

	FY 2023 Engagements			*FY 2022*
Audit Firm	***Audit Fees***	***Non-Audit Fees***	***Total Fees***	