LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Miki Cestnik, Information Systems Audit Manager

CC:
Office of the Commissioner of Higher Education
Clayton Christian, Commissioner of Higher Education
Tyler Trevor, Deputy Commissioner, Budget, Administration, and Planning
University of Montana
Seth Bodnar, President
Zach Rossmiller, Chief Information Officer
Montana State University
Dr. Waded Cruzado, President
Ryan Knutson, Chief Information Officer

DATE: September 2023

RE: Information Systems Audit Follow-Up (23SP-10): *Information Security in the Montana University System* (20DP-03)

ATTACHMENT: Original Information Systems Audit Summary

Introduction

The *Information Security in the Montana University System* (20DP-03) report was issued to the Legislative Audit Committee in March 2022. The audit included four recommendations to various entities of the university system. In July 2023, we conducted follow up work to assess implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

The Office of the Commissioner of Higher Education (OCHE) is the central administrative unit of the Montana University System (MUS) and the Board of Regents (board). The MUS has various campuses across the state split into two institutions: Montana State University (MSU), and the University of Montana (UM). To provide necessary services and education, universities gather and store various types of sensitive information related to students' education and personal information, employees' personal information, credit and bank account information, intellectual property, and personal health information. The audit reviewed how information system's security is governed and managed between the various entities and if each institution has mature procedures to manage security risks. We identified that the universities have struggled to mature their risk and security management for various reasons. OCHE and the board needed to provide clear direction about the governance structure for the universities to effectively make progress. Overall, our follow-up work identified significant changes implemented by OCHE and the board that have helped the universities make progress over the past year. Board policy and a formal governance structure with authority and communication have been established. Each university is undergoing a formal, comprehensive risk assessment to assist in implementing changes and growing security programs. The audit contained four recommendations: three are implemented and one is being implemented.

Background

The Montana University System (MUS) consists of various entities that must work together to ensure security of sensitive data. Montana state law defines activities that are required for maintaining information security throughout state government. However, state law excludes the university system from these requirements. Therefore, the Board of Regents (board) and Office of the Commissioner of Higher Education (OCHE) are responsible for governing information technology (IT) management practices and information security through the university system. Based on the security needs for higher education, the separation from the executive branch security operations and resources, and increase in threats, the audit objectives focused on the risk management procedures at each institution within the MUS and the overall structure of security governance.

We identified that while security activities occurred at each flagship campus, they struggled to mature the overall security program due to a lack of structure for authority, guidance, and communication. Each university had areas of improvement that were necessary as well, and a formal, comprehensive risk assessment needed to be performed to set a baseline for continuous improvement and assessment.

Audit Follow-up Results

Follow-up work reviewed the efforts of OCHE and the universities to establish a governance structure and the risk assessment each university conducted over the summer of 2023. It was apparent that the university system took the findings seriously and made a significant effort to formalize the governance and management of security throughout all campuses. Documentation of the changes and new structure have been adopted by the board and are outlined for the public on their website. The following sections outline the progress towards implementation of report recommendations.

Recommendation #1

We recommend that Board of Regents and the universities review and enforce university system security policy that includes:

A. Clear direction within policy to manage a security program and mandate a consistent security framework, going above and beyond maintaining security policies.

B. Requirements for Board of Regents security policy to be reviewed continuously.

Implementation Status – Implemented

At the time of the audit, the board had an incomplete and outdated security policy guiding the university system. It lacked specific guidance for the universities to implement a consistent approach, which hindered their ability to coordinate and strategically improve their security programs.

Since the audit, the board security policy has been updated to define a security framework and process for reviewing this policy continuously. This policy has been posted on the board website and both universities are currently using the framework to guide the improvements they are making in their security programs. Universities indicated the change has improved expectations and understanding of the security baseline they are measured against. This along with the structure of recommendation four will improve the university system's ability to enforce security standards as well.

Recommendation #2

We recommend the University of Montana:

A. Update and formalize job descriptions for positions that have responsibilities for developing, maintaining, or supporting the security program, and

B. Complete a comprehensive IT risk assessment that is used to develop strategic initiatives and the required budget to mature the security program and security awareness.

Implementation Status – *Being Implemented*

Our initial audit work identified that the University of Montana (UM) did not have the roles and responsibilities defined to manage security clearly established throughout IT. They also struggled with prioritizing and coordinating multiple areas of improvement through various leadership changes prior to the audit. Assessing the risks the university faces and defining the key roles in managing security improvements were necessary for UM to build a strategic roadmap and mature its security program.

In 2022, UM revised several key job descriptions to include explicit expectations for these roles in the security program, addressing part A of the recommendation.

In 2023, MUS contracted with an external vendor for a comprehensive assessment of IT security and specific federal regulations that apply to the universities. The contract included work at both universities. UM is currently waiting for the final report from the vendor and has already established how the results will be used to inform enterprise risk management efforts. The contract also included 40 hours of support from the vendor to implement changes. Integrating this assessment and the vendors support with risk management will help inform the strategic plan and budgeting process for the upcoming years. UM plans to have the next strategic plan with this information done by the end of 2023. UM indicated this assessment will also be part of future internal audit programs to ensure progress continues.

Recommendation #3
We recommend the Montana State University complete a comprehensive IT risk assessment to develop a formal approach for maturing security procedures.

Implementation Status – Implemented
Our initial audit work identified that Montana State University (MSU) had struggled with general IT staff turnover, which impacted its ability to progress the security program. MSU's larger problem was the lack of framework to measure their security program against and provide direction on what needed to be improved. Security frameworks help provide a structured approach to building a security program, while also giving a comprehensive set of standards to compare against.

Since the audit, MSU has implemented a cybersecurity framework. As part of the contract discussed in recommendation 2, MSU also had an assessment of IT security and federal regulation compliance completed. This assessment covered the security program in regard to the new cybersecurity framework and specific regulations that were reviewed during the audit. They received the final report at the end of August 2023. A cybersecurity incident did occur at the university this spring, prior to the final assessment report, but the university has recovered and is working to incorporate the lessons learned from the event with the results of the assessment to formalize a unified approach to making improvements. MSU indicated that the assessment will also be used for future reviews of the security program.

Recommendation #4
We recommend that the Board of Regents establish system-wide IT governance that ensures:
A. OCHE has an active role in improving security posture of the university system,
B. Security policy addresses the requirements of data security statute and other relevant federal requirements,
C. There is clear allocation of security responsibility, authority, and accountability, and
D. Communication and reporting mechanisms are formalized between various entities that oversee or make decisions within the university system.

Implementation Status – Implemented
At the time of our audit, the universities were struggling to mature security programs and needed guidance, support, and a clear understanding of roles and authority throughout the university system. As the administrative unit for the board, OCHE is responsible for providing this direction and clarity to the entire university system. Clear accountability, communication, and direction were not established at the time and all entities struggled coordinating and supporting each other.

Since the audit, OCHE has defined a governance and reporting structure that provides clear lines of authority and communication throughout the MUS, from OCHE to each affiliate campus. The two flagship campuses now have the ability to direct and manage the security functions of the affiliate campuses. This will allow for consistency, accountability, and support between all of the campuses within the institution. OCHE has also defined various roles and responsibilities as part of the governance structure. Important points of communication and coordination have been made more clear, such as the IT council and IT security steering committee. OCHE has also outlined the role of internal audit and enterprise risk management in regard to IT security which will improve decision making and accountability through the MUS. Overall, the universities have welcomed this clarity, even though there are initial challenges in ensuring the resources are available to support the change. Both UM and MSU have noted increased support and communication from the changes that have been made.