A Report
to the
Montana
Legislature

Information Systems Audit

Information Security in the Montana University System

The Montana Board of Regents
Office of the Commissioner of Higher Education
University of Montana
Montana State University

March 2022

Legislative Audit
Division

20DP-03

Fraud Hotline
(Statewide)
1-800-222-4446
(in Helena)
444-4446
LADHotline@mt.gov
www.montanafraud.gov

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives. Members of the IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee, which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Miki Cestnik	William Soller

Reports can be found in electronic format at:
https://leg.mt.gov/lad/audit-reports

LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller

March 2022

The Legislative Audit Committee
of the Montana State Legislature:

This is our information systems audit of information security management and practices managed jointly by the University of Montana, Montana State University, and the Office of the Commissioner of Higher Education (OCHE).

This report provides the Legislature information about the security programs at each university and security governance provided by OCHE. This report includes recommendations for each university to improve security programs and for the Board of Regents and OCHE to more directly manage security policy and governing structure with the university system. A written response from each university and OCHE is included at the end of the report.

We wish to express our appreciation to Montana University System personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Table of Contents

Figures and Tables

Figures

Tables

Elected, Appointed, and Administrative Officials

		Location	Term Expires
Board of Regents of Higher Education	Casey Lozar, Chair	Helena	February 1, 2025
	Loren Bough	Big Sky	January 31, 2027
	Todd Buchanan	Billings	January 31, 2028
	Joyce Dombrouski	Missoula	February 1, 2026
	Brianne Rogers	Bozeman	February 1, 2024
	Jeff Southworth	Lewistown	January 31, 2029
	Amy Sexton, Student Regent	Billings	June 30, 2022
	Clayton Christian, Commissioner of Higher Education*		
	Greg Gianforte, Governor*		
	Elsie Arntzen, Superintendent of Public Instruction*		

*Ex officio members

Office of the Commissioner of Higher Education	Clayton Christian	Commissioner of Higher Education
	Tyler Trevor	Deputy Commissioner for Budget and Planning, Chief of Staff
	John Thunstrom	Montana University System Information Technology Director
	Margaret Wallace	Director of Assurance and Enterprise Risk

Montana University System Campuses	Seth Bodnar	President, University of Montana
	Dr. Waded Cruzado	President, Montana State University
	Zachary Rossmiller	Chief Information Officer, University of Montana
	Ryan Knutson	Chief Information Officer, Montana State University
	Anta Coulibaly	Director of Internal Audit, University of Montana
	Ila Saunders	Interim Director of Audit Services, Montana State University

Report Summary
Information Systems Audit 20DP-03 March 2022
Montana Legislative Audit Division

Information Security in the Montana University System

The Montana Board of Regents, Office of the Commissioner of Higher Education, University of Montana, and Montana State University

Background

In Montana, the governance and administration of the Montana University System (MUS) is vested with the Board of Regents (board), which has the power and authority to supervise, coordinate, and control the Montana University System. The Office of the Commissioner of Higher Education (OCHE) is the central administrative unit of the Montana University System and the Board of Regents. The Montana University System comprises of 16 public universities and colleges, enrolling more than 40,000 students each semester.

Each major campus has several affiliate campuses across the state. Campuses split into two institutions: Montana State University (MSU), and the University of Montana (UM). Community colleges and Tribal colleges are independent institutions. OCHE provides guidance and direction to each institution and the independent institutions. Each campus maintains independent administration with some shared services.

The universities have struggled to develop security programs and risk assessment procedures. OCHE and the Board of Regents have not established a direction with the clear roles and responsibilities needed to support university security programs and enforce strong security practices. While each university faces different challenges in making progress to ensure university data is protected, each needs to address risks through a comprehensive IT risk assessment. This will help prioritize efforts to address staffing, compliance regulations, and formalizing security practices.

KEY FINDINGS:

Board of Regent policy does not mandate a security framework to define security program guidance. OCHE intended to give the universities leeway to decide what exact framework would work best to direct security operations. However, this has caused the universities to not adopt a formal framework or set of frameworks. The lack of framework has contributed to the absence of a mature security program structure and has slowed progress in developing security programs at each university.

Each campus needs to make progress towards a structured security program. OCHE has delegated responsibility for managing a security program to each university. Each university is spending valuable time reacting to the effects of risks as opposed to proactively assessing risks. Both universities are working towards better planned security practices, and each university needs to improve in key areas like information security policies and risk assessment.

Governance needs to be strengthened to support security programs. The Board of Regents and OCHE are responsible for defining governance that directs security practices throughout the university system. However, policy does not ensure the minimum security requirements within state law are met, informal coordination and communication between various entities does not ensure informed decisions and knowledge sharing, and the location and responsibilities of security staff needs to be reviewed to best support communication, decision making, and accountability for security practices.

(continued on back)

For the full report or more information, contact the Legislative Audit Division.

leg.mt.gov/lad

Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705
(406) 444-3122

The mission of the Legislative Audit Division is to increase public trust in state government by reporting timely and accurate information about agency operations, technology, and finances to the Legislature and the citizens of Montana.

To report fraud, waste, or abuse:

Online
www.Montanafraud.gov

Email
LADHotline@mt.gov

Call
(Statewide)
(800) 222-4446 or
(Helena)
(406) 444-4446

Text
(704) 430-3930

RECOMMENDATIONS:

In this report, we issued the following recommendations:
To the Board of Regents: 2
To University of Montana: 1
To Montana State University: 1

Recommendation #1 (page 11):
Security Framework Management
The Board of Regents needs to work with the universities to determine which framework to adopt and incorporate into board policy.

Board response: **Concur**

Recommendation #2 (page 14):
Risk Assessment and Security Strategy
The University of Montana needs to develop a strategic road map and clearly define the role of key security staff to be able to improve their security program. This strategy needs to be supported by a comprehensive risk assessment to communicate and prioritize the risks the university is facing.

University response: **Concur**

Recommendation #3 (page 15):
Structured Security Approach
Montana State University needs to formalize the approach for maturing their security and risk management programs. This will help to prioritize the work to document and evaluate the security program.

University response: **Concur**

Recommendation #4 (page 22):
Security Governance
The Board of Regents needs to define OCHE's role in IT governance and how they support security in the MUS; direct universities through stronger policy; clearly allocate security responsibility, authority and accountability; and define the communication structure to support strong governance.

Board response: **Concur**

Chapter I – Introduction, Scope, and Objectives

Introduction

The Montana University System (MUS) comprises 16 public universities and colleges, enrolling more than 40,000 students each semester. The governance and administration of the MUS are vested with the Board of Regents (board), which has full authority to manage and control the MUS. Before 1994, the university system was comprised of independent campuses that reported to the board. In 1994, the system was restructured to coordinate campuses with the additional oversight of the Office of the Commissioner of Higher Education (OCHE). OCHE is the central administrative unit of the MUS and the board. In addition, OCHE supervises and coordinates other public educational institutions assigned by law.

These public universities are split into two institutions: Montana State University (MSU), and University of Montana (UM). Each institution consists of a major campus, MSU in Bozeman and UM in Missoula, with a network of several affiliate campuses across the state. OCHE provides guidance and direction to each institution; however, they each are administered independently with some shared services between the two.

Information Security Within Higher 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. This type of sensitive data requires controls that maintain information security. The most notable information security requirement for higher education is the Family Educational Rights and Privacy Act (FERPA) that protects the disclosure of students' educational records. In the context of higher education, personally identifiable information (PII) can include student names, mothers' maiden names, social security numbers, identification numbers, or parent/guardian information.

Higher education institutions also hold financial and intellectual information that are subject to federal security requirements.

- Universities are required to safeguard customer financial information according to 16 CFR Part §314, known as the Gramm-Leach-Bliley Act (GLBA), due to their participation in financial loan activities. In addition to the disclosure of student information, this act also requires the security and confidentiality of customer information, protection against anticipated threats to security, integrity, and unauthorized access or use of the information.
- Universities also manage federal information for research purposes or carrying out the work of federal agencies, such as the Department of Defense. The requirements are to ensure federal data is protected when it is processed, stored, or used in nonfederal information systems. The requirements are comprehensive, and depending on the data being shared, universities will need a federal certification that shows mature control structures. The controls outlined are grouped into various families including basic practices, such as access control, user awareness and training, incident response, and risk assessment.

Montana Information Security Requirements

Montana state law also defines activities that are required for maintaining information security throughout state government. The Department of Administration (DOA) and the State Information Technology Services Division (SITSD) ensure these laws are met across the state network, but educational agencies are excluded. Section 20-32-101, MCA, establishes an educational telecommunications network for instructional and educational coursework of students from kindergarten through higher education as well as any supporting information to teachers. As result of this, the MUS and agencies involved in educational services have their own telecommunication network separate from other executive agencies. Therefore, DOA and SITSD do not have authority or provide direction over MUS IT or security.

The board and OCHE are responsible for governing IT management practices and information security through the university system. Section 20-25-301, MCA, outlines the powers and duties of the board, including that the board shall ensure an adequate level of security for data within the university system by addressing state law information security requirements. These requirements are further defined in §2-15-114, MCA, and direct agencies to develop and maintain policies and procedures to ensure information security, ensure an individual is responsible for a security program and safeguards, and conduct internal evaluations of the security program for improvements.

While the MUS has this direction within state law, they are not under the authority or security governance established by SITSD through Montana Operations Manual policy. Therefore, a separate governance and security structure needs to be in place to fit the needs of MUS. Board duties and federal requirements also require this structure to be in place for comprehensive security and mitigation of risks that face higher education.

Audit Scope and Objectives

Over the past few decades, there have been multiple breaches at higher education institutions. These breaches have resulted in the loss of student data, employee data, intellectual property, credit and bank account information, and personal health information. With the increased threat to higher education data, and increased security requirements from federal entities, it's crucial for university system security programs to be well-defined and comprehensive so they can improve and adapt to evolving security risks easily.

Prior audit work for the MUS has focused on Banner, the system that manages student data and other shared IT services. During reviews, we identified that a higher-level security management review at MUS was needed due to the changes to risks the universities are facing. Based on these security requirements for higher education, the separation from the executive branch security operations and resources, and increase in threats noted above, the objectives of this audit included:

1. Determine if the Montana University Systems have mature risk management procedures that ensure university data is protected.
2. Determine if the current security governance structure provides security guidance and accountability through internal evaluations of security policies and procedures.

The scope of this audit included the current governing structure of policies, procedures, authority, and accountability required by OCHE, as well as the security practices and policies at both major campuses within the two university networks, UM Missoula and MSU Bozeman. Security programs for affiliated campuses were not reviewed due to the size difference in student enrollment. Affiliated campuses are also expected to use the network managed by either UM or MSU and rely heavily on their respective university to provide IT support and direction.

Audit Methodologies

Audit methodologies included:

- Assessed maturity of key aspects of each university's security program and inclusion in risk management.
- Contracted with an outside consultant with experience in security testing and phishing campaigns to review security vulnerabilities and security awareness at MSU and UM. The results of this work have been omitted from this report. This information could be used by malicious actors to attack or harm the universities.
- Identified governance and staffing structure directing security programs at OCHE and each campus to identify roles and responsibilities.
- Discussed accountability under the governance framework and identify controls needed to maintain communication and consistency of a solid security program.
- Discussed security program resources with both OCHE and universities.
- Reviewed other state university system support structures to identify characteristics that Montana may need to consider in determining solutions.

We also compared key aspects of each university's security program and the governance structure in place to industry standards where appropriate. Industry standards included:

- **National Institute of Standards and Technology (NIST):** Provides a catalog of security and privacy controls for information systems. These publications used in our audit address frameworks for cybersecurity and risk management, and standards for common security controls. NIST publications are suggested in board policy and are used to certify security control maturity needed for upcoming Department of Defense contracts.
- **Control Objectives for Information and Related Technology (COBIT):** Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks. OCHE is using COBIT to guide decisions for roles and responsibilities in the MUS.
- **EDUCAUSE:** Nonprofit organizations exist to assist universities with securing information by providing tools, examples, and assistance specific to higher education needs. For our work, we chose the nonprofit EDUCAUSE geared towards technology and assisting higher education with the implementation and management of information technology.

Chapter II – Campus Information Security Programs

Introduction

The Montana University System maintains various types of sensitive information that require strong security controls. Higher education has been a target for external attacks due to the wealth of information. State laws exist to provide authority and require action to prevent such attacks; however, it is the actions of each individual campus that are the most significant in reducing risk of data breaches, data loss, or noncompliance with federal requirements that could result in loss of funding.

The Office of the Commissioner of Higher Education (OCHE) has delegated to the major campuses the authority to administer their own information network, leaving this responsibility to the University of Montana (UM) and Montana State University (MSU). As a result, campuses have the individual responsibility to assess their IT environments and security programs for various risks from external threats, weak controls, and compliance with state and federal requirements.

During initial fieldwork we identified that risk management processes within IT were not consistent or comprehensive at either university. Therefore, the overall security program at each campus needed to be evaluated to understand the impact of underdeveloped risk management procedures.

Assessing Security Programs Is a Common Practice With Various Tools Available

Industry standards provide many tools and guidance on assessing security programs. For our work, we chose an assessment tool that was developed for higher education. The tool assesses high-level, common security practices shown in Figure 1 (see page 6).

Figure 1

Security Program Assessment Areas

Security Program Assessment Areas

Multiple practices within each area assessed for maturity

15 Control Areas

- Risk Management
- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Aspects of Business Continuity Management
- Compliance with Necessary Requirements

Source: Compiled by the Legislative Audit Division.

The assessment tool we used includes specific practices in each area for maturity to be assessed. The tool summarizes maturity into six progressive levels, starting with security practices that don't exist and do not have plans in place, moving to mature security practices that are measured and monitored to assess efficiency. Table 1 defines the levels of maturity used to describe the security programs at each campus.

Table 1

Security Program Maturity Levels

Score	Maturity Level	Definition
0	Not Performed	There are no security controls or plans in place. The controls are nonexistent.
1	Performed Informally	Base practices of the control area are generally performed on an ad hoc basis. There is general agreement within the organization that identified actions should be performed, and they are performed when required. The practices are not formally adopted, tracked, and reported on.
2	Planned	The base requirements for the control area are planned, implemented, and repeatable.
3	Well Defined	The primary distinction from Level 2, Planned and Tracked, is that in addition to being repeatable the processes used are more mature: documented, approved, and implemented organization-wide.
4	Quantitatively Controlled	The primary distinction from Level 3, Well Defined, is that the process is measured and verified (e.g., auditable).
5	Continuously Improving	The primary distinction from Level 4, Quantitatively Controlled, is that the defined, standard processes are regularly reviewed and updated. Improvements reflect an understanding of, and response to, a vulnerability's impact.

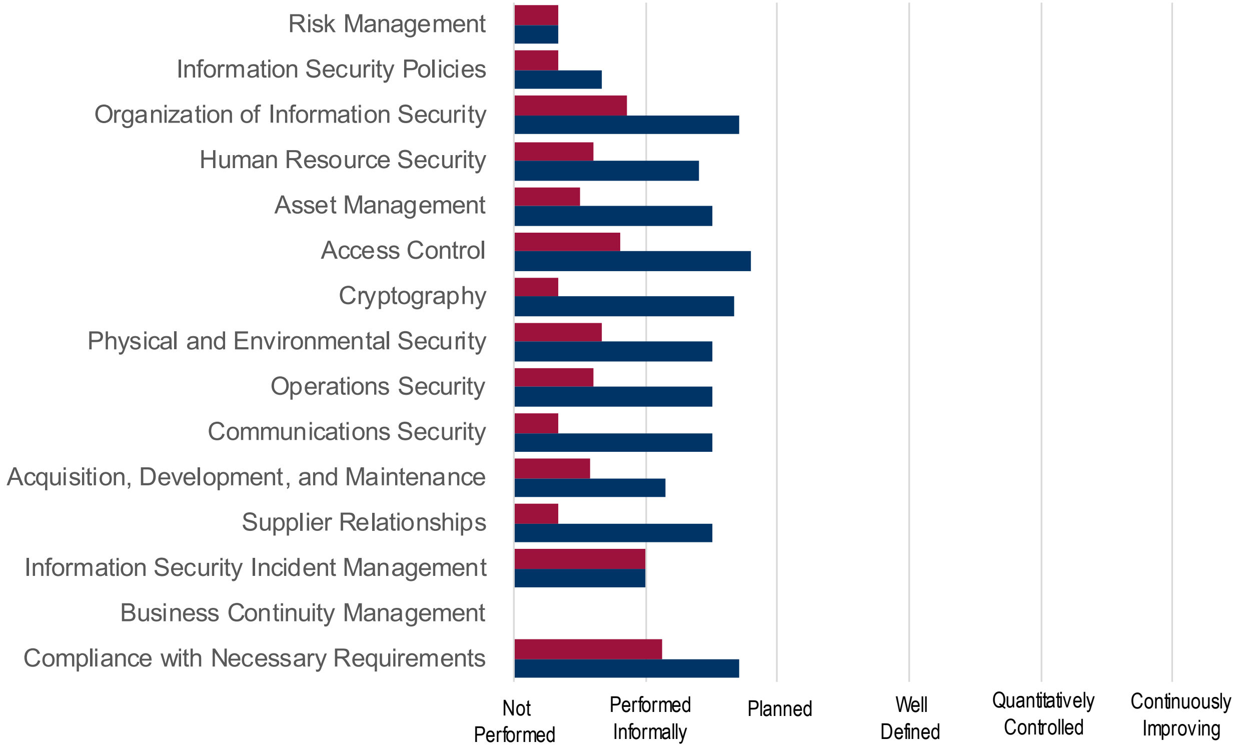
Source: EDUCAUSE Security Program Assessment Tool.

Security Assessments Indicate Progress Needs to Be Made

Each university's security program is at a lower maturity level. Figure 2 shows that improvement is needed in each area of best practice for both universities.

Figure 2

University Security Assessment Results for University of Montana and Montana State University



Source: Compiled by the Legislative Audit Division.

While this assessment does not include all control practices in each area, it does review some of the more important controls that contribute to a thorough security program. For instance, both universities scored low in Business Continuity Management. The assessment examines how well-documented the plan for continuing business is, the analysis that informs the plan, the testing and understanding of the plan, and approval of the plan. While this level of control wasn't present at either university, it does not mean other controls related to business continuity are not present, such as data backup and incident response. However, what is absent is how those other controls mitigate the risks the university faces without a plan that comprehensively documents the actions needed to respond to a disruption.

Additionally, both universities scored low in risk management. A high score indicates that a formal risk management program addressing IT risks is documented, thorough, and includes routine assessments to identify key objectives that need to be addressed within the security program. These specific practices were not mature during our assessment; however, it does not mean that the universities are not reacting to risks. They are making progress where they can as issues arise, but what was not evident was a formal program that continually assesses the coverage of IT controls that do exist and the IT risks that each university faces.

Each university is in a place where they are spending valuable time reacting to the effects of risks as opposed to proactively assessing risks. This has created varying maturity levels across the university system. Critical practices like risk management, although resource-heavy, need more attention.

Each Campus Faces Risk Without Progress in Maturing a Security Program

For either campus, security incidents will always be a risk to prepare for. However, the campuses also need to make progress in maturing security programs to mitigate risks of noncompliance that can impact the financial situation of each university. More specifically, each university's ability to obtain cybersecurity insurance and meet various federal requirements for federal funding and contracts is affected.

Cybersecurity Insurance: This insurance protects an organization against the financial loss caused by cyber incidents, like data breaches. It is important as the cost of cyber incidents can be significant, and general insurance policies do not cover this kind of situation. Like general insurance policies, an assessment is done on a consistent basis to identify the needs and costs of cybersecurity insurance based on the magnitude of risks and likelihood an incident will occur. Various cybersecurity insurance policies exist. These range from general cybersecurity to other types of liabilities that may have more specific fines, such as Health Insurance Portability and Accountability Act (HIPAA) data liabilities.

Before 2021, the state purchased two separate cybersecurity insurance policies for state agencies–one general cybersecurity policy and another specifically designed to cover cyber incidents related to HIPAA.

In 2021, UM received a quote of $44,000 from an alternative insurance company for HIPAA specific cybersecurity insurance. This was after their previous insurance provider refused to renew the policy because the security program at UM posed too much risk. The new quote represented a 300% increase in cost from the previous year ($11,000) and was accompanied by a $100,000 deductible without the additional coverage the previous insurance offered. After consulting with the state's chief Risk Officer, UM declined this offer and forwent HIPAA-specific cyber security coverage. UM continues to be covered by the state's general cybersecurity insurance policy. While there is no specific feedback on why an insurance carrier would increase the cost of insurance, the information provided in the insurance assessment and the rising costs of cybersecurity insurance are both factors in determining the proposed policy.

Federal Requirements: Both universities have to comply with security requirements of financial institutions and to be considered for research contracts from the Department of Defense (DOD). Based on our assessment of the security programs, neither campus is fully complying with financial institution requirements and have significant progress to make to become certified for DOD contracts. Current DOD contracts are not affected; however, if the universities wish to pursue this type of funding in the future, they need to make improvements now.

Security Framework to Guide Campuses Is Not Mandated

While both universities need to make improvements to security programs in different ways, some of the causes go beyond what the universities are responsible for. As the oversight for the Montana University System, the Board of Regents (board) and the Office of the Commissioner of Higher Education (OCHE) need to fully understand their role in mitigating risks that can significantly affect one or both universities. They play a key role in moving the security programs at each university from planned practices to a well-defined maturity where the practice is not only repeatable, but documented, approved, and implemented across the entire university.

State law assigns the board the responsibility of ensuring an adequate level of security for data within the Montana University System. Board policy is meant to clarify how this statute is carried out and states that "Where appropriate, campuses should follow the National Institute of Standards and Technology (NIST) Framework for policy guidance." While OCHE intended to give the universities leeway in deciding on what exact framework would work best, the language chosen has caused the universities to not formally adopt any framework to guide their security programs. The lack of framework has contributed to the current state of security programs and has slowed progress in development.

Board Policy Needs to Be More Direct About Security Frameworks

As the entity directed to ensure security, the board and OCHE are responsible for governance and policies that guide the frameworks in place for the university system. This governing policy should create consistency and be explicit about the high-level procedures to maintain a security program. Each university can determine more specific policies around controls and how they are managed as they also need to consider business differences.

The current board security policy has not been reviewed since 2014. This direction requires consistent frameworks to be established considering leadership changes and the desire to be consistent for resource sharing between the universities. However, OCHE needs to work with the knowledgeable university staff to determine which framework or blend of frameworks to guide IT and security and incorporate into board policy. This process should also be done continually as security frameworks and standards evolve to meet new risks.

Being more explicit in governing policies will provide the universities the direction and structure they need to improve their security programs. It will also create accountability to ensure improvements are made and federal requirements are satisfied.

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.*

Each University Has a Responsibility to Maintain Their Security Program and Make Improvements

While OCHE's limited direction for universities has contributed to the state of each security program, OCHE is not solely responsible for either security program. Each university must also play a role in managing its security program. OCHE's delegations have given each university autonomy to govern and manage security how they see fit. However, this has created a more significant obstacle for each university to address. Without guidance, the success at each university relies on its staff to create governance and address individual university challenges. Both universities are making progress but need to focus on their improvements if they are going to move forward developing comprehensive security programs and further securing student information.

Results of Contractor Testing Show Control Weaknesses

We contracted with an outside consultant to conduct testing and run a phishing campaign at each university. This testing identified specific vulnerabilities and showed what security weaknesses could be exploited if identified by a malicious actor. The phishing campaign included an email we crafted to look like a survey from the IT department. This test informed us of the level of security awareness among university staff.

The findings of these tests were classified, according to industry standards, as high, medium, or low concerns. From testing, each university had two high concerns and five moderate concerns found in testing. For the phishing campaign, UM results were rated as a high concern and MSU was rated as a low concern when compared with similar organizations.

All findings were shared with each university. Both indicated progress towards resolving the issues identified; however, there is still work that needs to be done to resolve high concern findings.

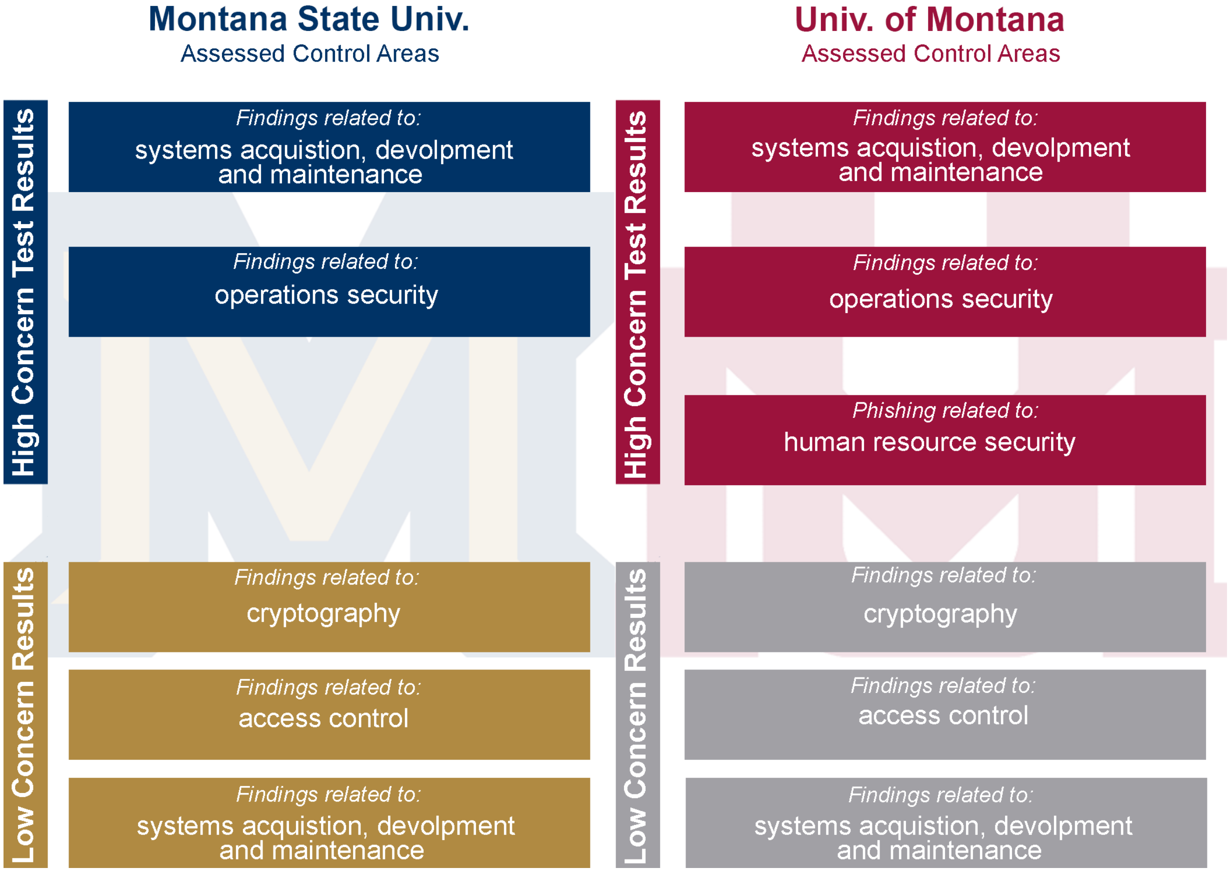
Security Weaknesses Are Mitigated by Control Areas Assessed

While the work of our contractor identified vulnerabilities, these findings should be mitigated by practices we assessed in the security program of each university. Our work reviewed the maturity of controls within 15 areas. In general, these controls are intended to mitigate specific risks the universities face, such as network penetration or virus infection. The contractor's work identified vulnerabilities where the control structure does not completely mitigate a specific risk. The contractor then used tools to identify if any of the vulnerabilities could be exploited. When vulnerabilities are exploited, they give valuable information or access for someone to further develop an attack plan, such as ransomware or data theft.

Figure 3 shows the areas of our assessment that include controls related the testing findings. From our assessment results, most of the controls that would mitigate the findings of testing are performed informally.

Figure 3

Assessed Control Areas Related to Testing Findings



Montana State Univ.
Assessed Control Areas

High Concern Test Results

Findings related to: systems acquistion, devolpment and maintenance

Findings related to: operations security

Low Concern Results

Findings related to: cryptography

Findings related to: access control

Findings related to: systems acquistion, devolpment and maintenance

Univ. of Montana
Assessed Control Areas

High Concern Test Results

Findings related to: systems acquistion, devolpment and maintenance

Findings related to: operations security

Phishing related to: human resource security

Low Concern Results

Findings related to: cryptography

Findings related to: access control

Findings related to: systems acquistion, devolpment and maintenance

Source: Compiled by the Legislative Audit Division.

The maturity level of these areas needs to improve to prevent the vulnerabilities identified from reoccurring and being exploited. Possible outcomes could be data breaches or ransomware attacks that impact university reputation and could stop the universities from providing services to students.

While each university is aware of the effects and is working to address the vulnerabilities, they have each faced different challenges in making more broad-level progress while reacting to various individual problems as they occur.

Leadership Changes Have Slowed Progress for University of Montana Security Program

Consistent leadership and strategy are necessary to create a culture of security and champion security initiatives. UM's IT division has had multiple changes and temporary staff since 2018. Management is also responsible for ensuring sufficient resources are available for a security program, and that roles and responsibilities are clearly defined. Throughout these changes in management and leadership, responsibilities related to security have not been defined or documented officially for all security related positions. Key security roles at UM varied in their level of documentation, including a job description that was being updated, a job posting, and an inaccurate job description. Without this clarity, UM's security program lacks accountability and understanding of expectations in some areas. This also limits enforcement to ensure staff complete necessary tasks that meet the needs of the security program.

UM has not been able to hire a permanent position to be accountable for a comprehensive security program either. In recent attempts, they have struggled to bring someone in who is willing to progress a security program from a low maturity level.

Without consistent, committed leadership and a strong security program, it has been hard to establish a culture across the entire university that values and supports security initiatives. OCHE and university leadership direction is important to bring security awareness and support across the entire university system. While staffing changes and administration changes are expected, if a mature security program were in place and the culture was there to support security, these types of changes wouldn't have such an impact on security.

University of Montana Needs to Strategically Develop a Security Program

While security staff and the CIO can take the initiative to create the security program for their organization, if it is not consistent with the universities' overall culture, a security program is difficult, if not impossible, to develop.

UM staff indicated a commitment to resolving security issues and doing whatever is necessary to support security program progress. They have developed security initiatives for 2022 that include improving the adoption of multi-factor authentication across all UM campuses, risk mitigation programs, security awareness campaigns, and identity management.

There is a clear drive to get this work done from within IT; however, staff feel that budgeting and resources are the challenge they are now faced with. While this may be a valid concern, if information security risks are not clearly communicated, resources and buy-in for these initiatives are still not guaranteed.

Previous efforts to include information security risks have not been based on a mature security program or IT risk assessment process guided by a comprehensive framework. Therefore, the information provided for enterprise risk management wasn't complete enough to understand the issues within

IT. Without complete and detailed information that is supported by a mature process, enterprise risk management cannot account for the risks the university system faces appropriately, such as noncompliance with federal information security requirements and potential fines for security incidents. A comprehensive IT risk assessment should include the scope of the entire security program under the guidance of the framework that is directed by board policy.

The university has worked to develop an Enterprise Risk Management program that reviews risks to strategic objectives, and an IT-specific risk assessment is needed to provide accurate and complete information for that process. UM can make informed decisions about information security risks and noncompliance to prioritize IT and security initiatives with this information. Strategic planning for security will develop a road map for this progress and identify UM's initiatives; however, university leadership and OCHE's involvement in these plans are necessary to support a culture of security across the university system and different organizations across the campus.

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.*

Montana State University Has Lacked Structure While Developing a Security Program

Staffing changes haven't affected MSU in the same ways as UM, however, staff indicated that overall IT staffing challenges have impacted the progress of the security program. Which shows in the maturity of MSU's security program. MSU staff indicated that the struggles of communication and priority are not impacting the progress of the security program. It appears that this consistent leadership has contributed to a culture that understands security across the campus and affiliates.

While this culture is critical in supporting a security program, guidance for what activities should be in the security program and how it should operate were still lacking. This guidance is found in a security framework. MSU had not formally adopted a security framework at the time of the audit. Therefore, MSU has lacked a structured approach in identifying where resources and effort should be focused to make strategic improvements. This has created a situation where there are areas of varying maturity within their security framework, from nonexistent to formally adopted controls. Without a structure that guides security practices, it is hard to ensure overall, comprehensive security exists and evaluate it for improvements.

Comprehensive evaluations of the risks that MSU faces are critical to the maturing the security program. A comprehensive IT risk assessment should include the scope of the entire security program under the guidance of the framework that is directed by board policy. MSU does not have a formal risk management process within IT. They contracted outside help for a risk assessment in 2018, but the risk assessment only addressed the Banner system. While Banner is the primary system for student information at the university, it is only one application within IT operations at MSU. A risk management program within IT needs to be established to better identify and articulate risks to all IT operations within MSU.

Montana State University Needs Well-Defined Risk Management Procedures

Industry-based security frameworks exist to provide this direction and guided approach. The lack of framework adoption was recognized in the risk assessment from 2018 and continues to be a point of concern that needs to be addressed by MSU. MSU staff indicated they are making progress towards a more structured security approach and working with OCHE and UM to define a system-wide security framework. A security framework can also help MSU continually assess IT risks to identify gaps, prioritize work, and determine if additional resources may be needed. The information from this assessment can help the university communicate risks, develop strategies, and assist the entire university system to meet various federal requirements and mitigate future risks.

Recommendation #3

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

Chapter III – Security Governance

Introduction

Security governance is the policies, procedures, and processes to ensure the organization's regulatory, legal, risk, environmental, and operational requirements are met. Security governance activities include:

- Establishing and communicating organizational cybersecurity policy,
- Ensuring cyber security roles and responsibilities are coordinated and aligned between internal roles and external partners,
- Regulatory requirements are understood and managed, and
- Governance and risk management processes address cybersecurity risks.

Security governance and the activities noted above need to be in place to reduce the risk staffing changes posed to the Montana University System (MUS). The security programs are not strongly directed from a centralized perspective, and therefore rely on the individuals at each university to go above and beyond. While the MUS has individuals who have started this, a security program will struggle to mature if it is based on the actions of individuals and not a structure of governance.

OCHE's Role in Security Governance

State law states that the Board of Regents (board) "shall ensure an adequate level of security for data…" As the administrative unit for the board, the Office of the Commissioner of Higher Education (OCHE) has the responsibility to make sure this happens. However, because the universities are self-administered, they also are responsible for securing data. This initial structure aligns with industry standards, where a board ensures various IT management practices like this occur. Chief executive officers, chief information officers, and business executives are responsible for getting the work done to create the intended outcome.

Currently, OCHE has established a board policy for information security that defines the responsibility of each university to maintain data security. However, the governing practices that OCHE is responsible for to direct and assist the universities in security data is not well defined. OCHE needs to direct these key practices to support the universities' efforts to progress their security programs, while also holding the universities accountable and ensuring communication between all entities.

Strong Security Needs Overall IT Governance to Be Established

Security programs are easier to implement when foundational IT governance exists because similar, basic practices have already been established. Without the foundational governance practices, it is less likely that comprehensive security programs can be built or will be able to adapt to various risks, such as leadership changes, evolving cybersecurity risks, and increasing federal requirements. Like strong security governance, strong overall IT governance includes:

- Having strong organizational policy,
- Clearly defined and coordinated roles and responsibilities throughout the organization,

- Mature risk management procedures at an organizational and IT level, and
- Consistent direction, monitoring, and evaluation of management practices for improvement.

In previous work related to shared services in the university system, our office recommended OCHE adopt an IT governance framework to help build these foundational governance practices. During our audit fieldwork, OCHE was in the process of implementing that recommendation and working to determine where accountability and responsibility belong throughout the university system. OCHE is using the Control Objectives for Information and Related Technology (COBIT) framework to guide this process.

OCHE Is Responsible for Defining Governance That Directs Security Practices

The security practices that need to be outlined by OCHE security policy are defined in state law. At a minimum, these include the development of policies and procedures, designating an information security manager, implementing safeguards, and ensuring internal evaluations of the security program are conducted. To be able to do this, OCHE needs to:

1. Define the security governance structure and direct how university system data security is governed. Specifically, OCHE should be managing policy set by the board to ensure it aligns with statute and defines responsibilities for securing data, so each university has direction and a clear understanding of their expectations. COBIT standards also indicate policy should drive the control expectations, be evaluated yearly, and ensure that procedures are in place to track compliance and define the consequences of noncompliance.
2. Ensure coordination and communication exist to inform policy decisions and security planning between the universities and OCHE. This is essential for sharing services, security approaches, and the benefits of continuous security improvements.
3. Establish the location and responsibilities of security staff among universities and OCHE to coordinate and support the policy decisions and communications noted above.

Policy Does Not Meet Minimum Requirements

When comparing board policy to statute defining the responsibilities for securing data, we identified that board policy is missing key areas. These areas should define how OCHE provides guidance, holds universities accountable, and establishes communication with universities. The current policy aligns with statute by requiring policies and procedures be established and an individual be designated to do so. However, internal evaluations of the security program are not addressed within board policy.

Without addressing these statutes within policy, OCHE has not established a strong governing structure that is able to direct universities to securing information.

Communication Between OCHE and Universities Is Too Informal

Currently, a single FTE at OCHE is responsible for coordinating and communicating with each university regarding any IT matter. Staff from each university are also in contact with each other. However, these discussions aren't an intentional part of a communication plan or governance structure that ensures information is shared when needed, decisions are made with the appropriate stakeholders, or proactive discussions occur. While these meetings are occurring out of necessity, the universities' desires to coordinate informal discussions tend to be more reactionary and less effective. For example, OCHE security policy hasn't been updated since 2014. If formal communications were established to discuss security needs, risks, and governance in general, OCHE might have reason to review or update the policy more frequently.

Communication structures and plans are part of effective governance models. OCHE is working on defining the responsibilities for each action within the framework. However, OCHE has not put into place changes that implement the framework.

By establishing these practices within a governance framework, OCHE would create a culture of informed leaders that can support IT and better align IT practices and business goals. Furthermore, by providing formal lines of communications through councils or committees, OCHE facilitates a knowledge-sharing culture with appropriate stakeholders involved in decision-making. This type of culture is crucial in maturing security programs and understanding and informing cybersecurity risk management. If this structure were in place, security policy would be driven by knowledgeable staff based on risks specific to the system, and discussions would include stakeholders, the board, and OCHE to increase understanding of security.

<u>Location and Responsibilities of Security Staff Needs to Be Reviewed</u>

Currently, OCHE staffing does not include dedicated security responsibilities. According to board security policy, security responsibilities are expected to be established at each university. Currently, these staff dedicated to security are at each flagship campus. The smaller campuses do not have IT security staff.

Frameworks and best practices do not dictate where security roles and responsibilities should be assigned in a structure like OCHE's; however, whatever structure is determined, it needs to support the governance design and work with communication and decision-making processes. For example, OCHE may choose to keep the current structure and require all security roles and responsibilities be at the larger university campuses. In this case, they need to ensure that authority is clear with smaller campuses. If OCHE chooses to hire a university system chief information security officer, this role's authority and responsibilities would need to be clearly defined within the entire structure. This includes how this position supports and directs the universities and manages internal activities of OCHE for the same reasons. In either case, OCHE needs to define how communication between management and security staff ensures information is shared with OCHE and the board as they are making decisions that affect the university system.

Other State Governance Models Vary in Layout

Other state university systems were contacted and reviewed to understand if there is a consistent model for Montana to use. There is no consistent structure that stood out or best practice for how to allocate staff and responsibilities relative to security, overseeing security, or making decisions. What we identified though, is that central offices for higher education take more active rolls in guiding security practices at universities and establishing communication points.

The following table shows states that responded for information. Various other states were researched through websites and online information.

Table 2
Information Security Structure in Other States

State	University System Structure	Security Staffing	Communication Points
Montana	**Overseen by central office**	**At largest universities to support smaller campuses**	**Informal monthly meetings**
Maine	Overseen by central office	Centralized CISO/team only	Annual security report to Board
South Dakota	Overseen by central office	Centralized CISO/ team, security teams at universities	Network and Security Committee
North Dakota	Overseen by central office	Centralized CISO/ team, security teams at universities	Information Security Council
Wisconsin	Overseen by central office	Centralized CISO/ team, security teams at universities	Technology and Information Security Council

Source: Compiled by the Legislative Audit Division.

Key observations from these responses and other states researched showed most states had more guidance and specificity for security policy at the system level. Specific observations include:

- One state noted that the structure they have is good on paper. However, governance doesn't clearly define authority and accountability, so universities still operate independently and are inconsistent.
- Almost all states had formal security communication points.
- More centralized security and coordination seems to be the strategy for more efficiency when staffing and budgets are a problem.
- Roughly half of the states reviewed had central security staff fulfilling some kind of role, and most of those also had security staff at universities as well.

Based on reviewing other states, OCHE's current structure of security staff may work. However, without strong governance, or the clear allocation of responsibility, authority, and accountability, a decentralized structure without more guidance doesn't support strong security practices or help the universities mature their security programs.

Assessing Risks Is Challenging Without Clear Boundaries for University Security Programs

While OCHE commits to guiding the universities, they also make impactful decisions about authority and responsibilities, putting them in the role of directing governance. One FTE at OCHE is tasked with operational, management, and oversight responsibilities, leaving little time for establishing governance or coordinating security across an entire university system. The staffing, roles, and responsibilities need to be reviewed by OCHE, but with the direction established by the governance structure they have chosen.

Both universities identified concerns with coordinating multiple campuses with different resources and budgets. This challenge was also raised by other state's university systems that we reviewed. To overcome this challenge, OCHE needs to define the boundary of the security program within UM and MSU to manage and clearly state the authority each university has regarding that boundary. This is critical for the overall security posture of the university system, including the affiliate campuses.

Without this action, the entire university system faces challenges in progressing security programs. The security programs need to improve quickly, as both universities are facing federal requirements that need to be met to avoid reputational and financial risks discuss in Chapter II. For example, information security requirements were added the single audit objectives in July 2019. To complete this work, we verified the following:

1. The institution has designated an individual to coordinate the information security program.
2. The institution has performed a risk assessment that addresses the three required areas: employee training and management; information systems, including network and software design, information processing storage, transmission, and disposal; and detecting, preventing, and responding to attacks, intrusions, or other systems failures.
3. The institution has documented a safeguard for each risk identified from step 2 above.

We determined that the universities have individuals coordinating the information security program. However, it's unclear how affiliate campuses should be included in this work because the boundary of the security programs that each university manages is not clearly defined. After reviewing IT risk assessment procedures, we determined that the universities have not performed an IT risk assessment that addresses the three areas required. There is no IT formal risk management program, including documented safeguards, that supports the improvements and drives initiatives for a comprehensive security program that meets the intentions of the requirements. Therefore, the findings related to each campus's security programs will be reported as federal noncompliance for the student financial aid federal assistance program in the Single Audit report, anticipated to be issued in June 2022. OCHE needs to develop stronger policy and define the boundaries of security programs so that universities can move forward with effective IT risk management programs.

Governance Needs Strengthening to Support Security Programs

If OCHE chooses to guide universities rather than provide services or dictate the specifics of each security program, then the board needs to define how OCHE is involved in security governance, ensure statute is being met, and identify how they, as stakeholders, need to be informed on security throughout the entire system. The lack of this governance structure has contributed to the struggles in maturing security programs at each university and could make sharing IT services related to security more complicated. If each university addresses a problem differently, they lose the ability to share knowledge and services for efficiency. However, with a consistent approach, universities can coordinate on similar issues, share knowledge and expertise, and have a better chance at system-wide efficiency.

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.*

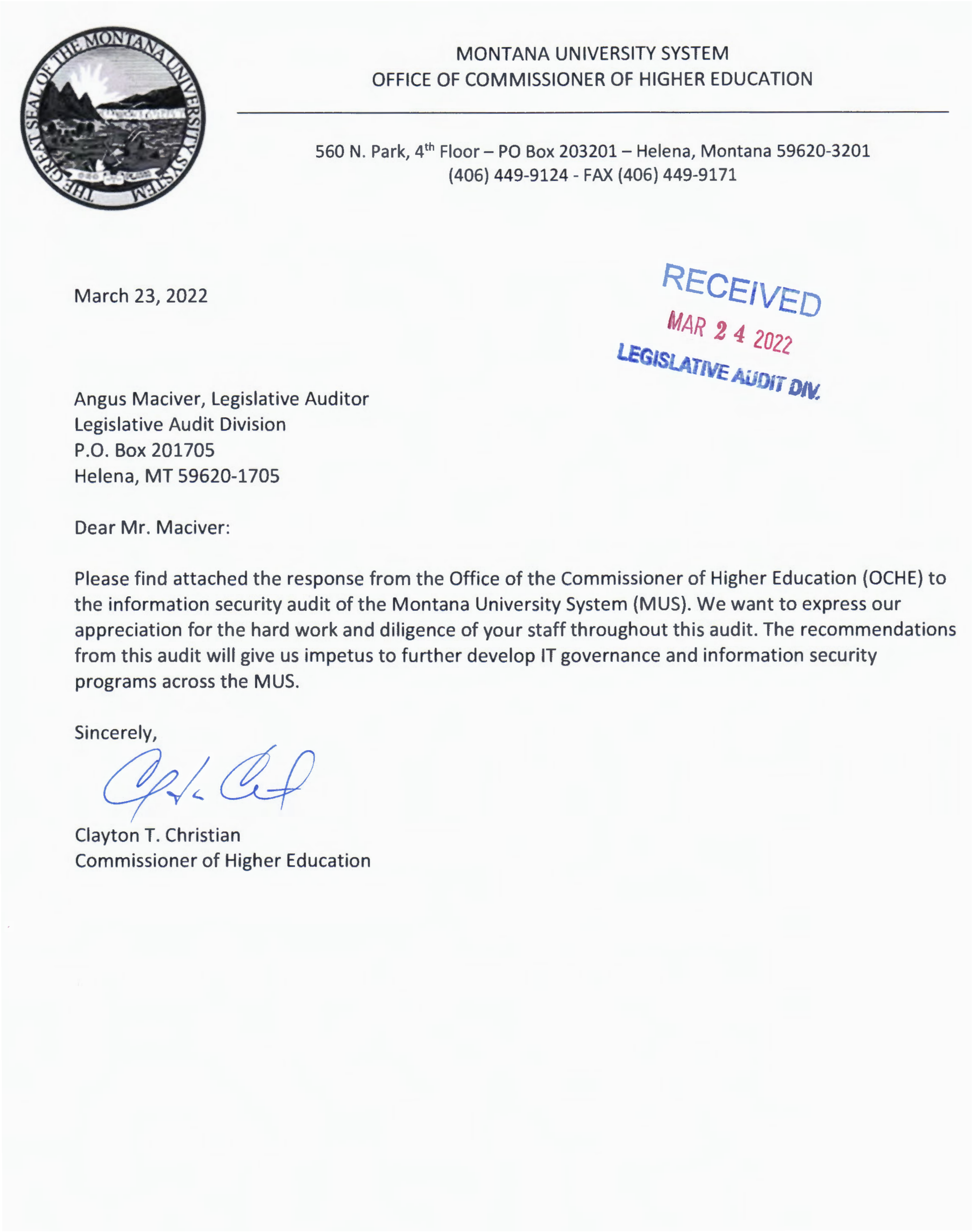
Montana Board of Regents

Office of the Commissioner of Higher Education

University of Montana

Montana State University

Responses



MONTANA UNIVERSITY SYSTEM
OFFICE OF COMMISSIONER OF HIGHER EDUCATION

560 N. Park, 4th Floor – PO Box 203201 – Helena, Montana 59620-3201
(406) 449-9124 - FAX (406) 449-9171

March 23, 2022

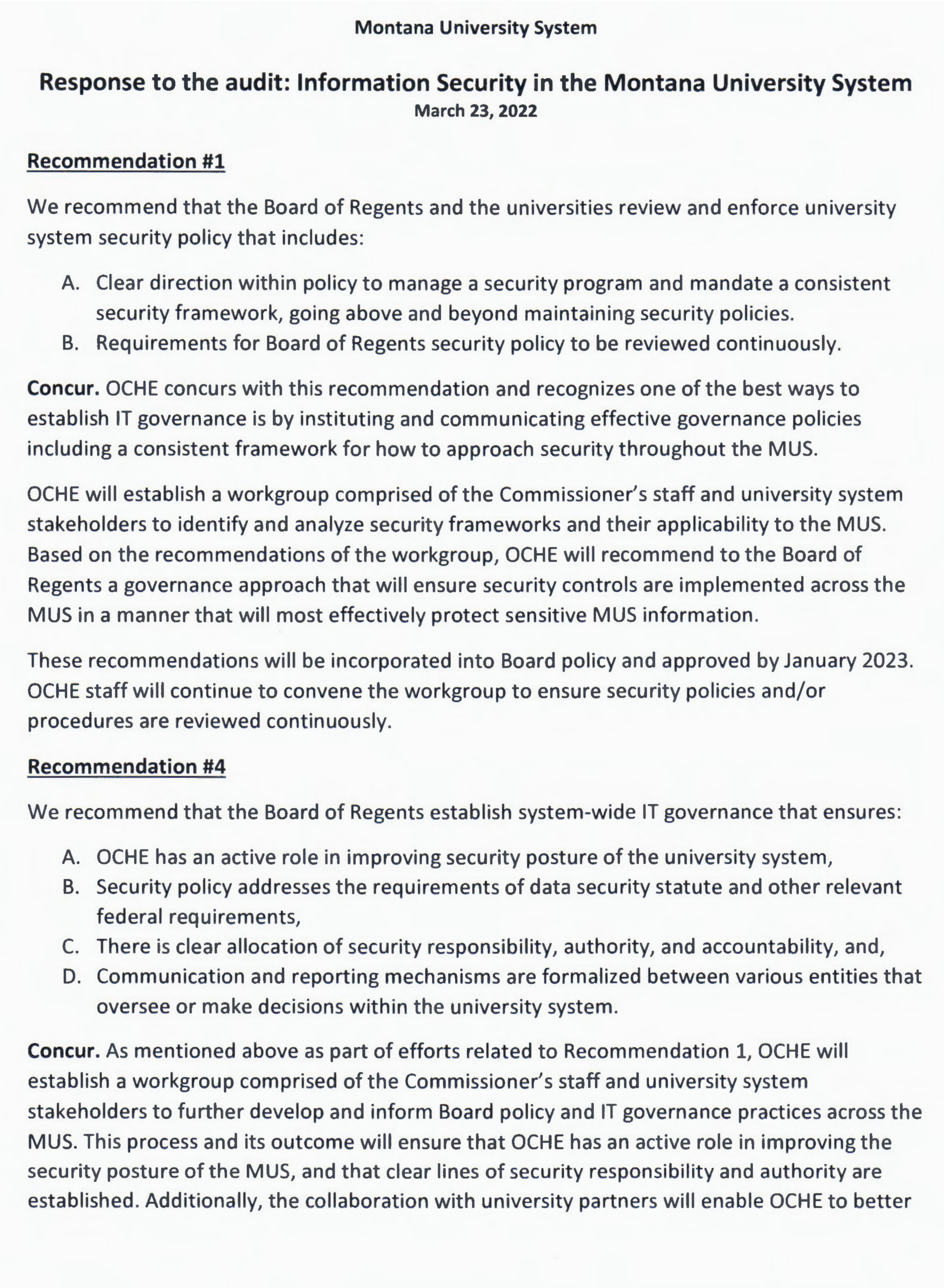
Angus Maciver, Legislative Auditor
Legislative Audit Division
P.O. Box 201705
Helena, MT 59620-1705

Dear Mr. Maciver:

Please find attached the response from the Office of the Commissioner of Higher Education (OCHE) to the information security audit of the Montana University System (MUS). We want to express our appreciation for the hard work and diligence of your staff throughout this audit. The recommendations from this audit will give us impetus to further develop IT governance and information security programs across the MUS.

Sincerely,

Clayton T. Christian
Commissioner of Higher Education



Montana University System

Response to the audit: Information Security in the Montana University System

March 23, 2022

Recommendation #1

We recommend that the 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.

Concur. OCHE concurs with this recommendation and recognizes one of the best ways to establish IT governance is by instituting and communicating effective governance policies including a consistent framework for how to approach security throughout the MUS.

OCHE will establish a workgroup comprised of the Commissioner's staff and university system stakeholders to identify and analyze security frameworks and their applicability to the MUS. Based on the recommendations of the workgroup, OCHE will recommend to the Board of Regents a governance approach that will ensure security controls are implemented across the MUS in a manner that will most effectively protect sensitive MUS information.

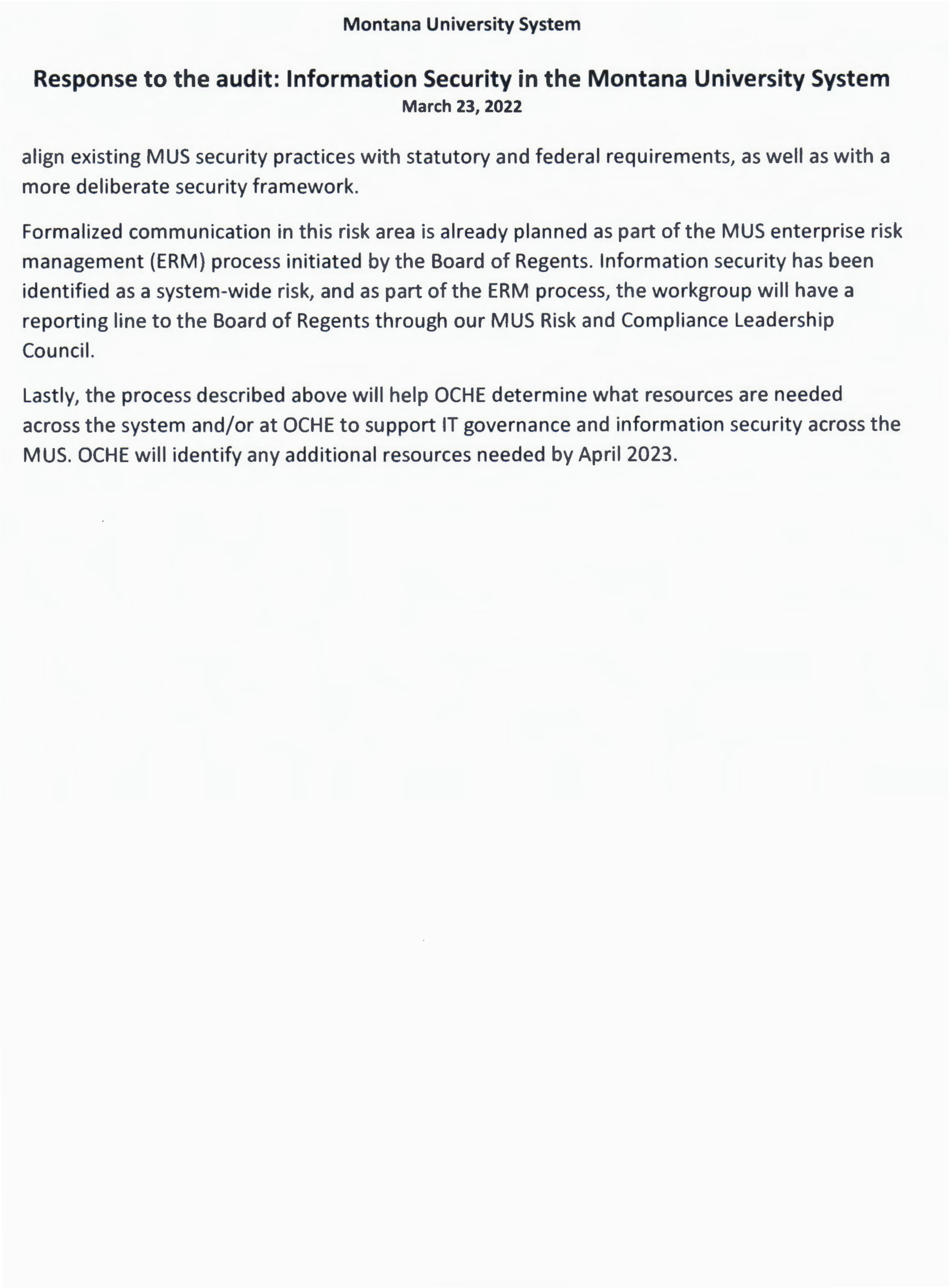
These recommendations will be incorporated into Board policy and approved by January 2023. OCHE staff will continue to convene the workgroup to ensure security policies and/or procedures are reviewed continuously.

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.

Concur. As mentioned above as part of efforts related to Recommendation 1, OCHE will establish a workgroup comprised of the Commissioner's staff and university system stakeholders to further develop and inform Board policy and IT governance practices across the MUS. This process and its outcome will ensure that OCHE has an active role in improving the security posture of the MUS, and that clear lines of security responsibility and authority are established. Additionally, the collaboration with university partners will enable OCHE to better



align existing MUS security practices with statutory and federal requirements, as well as with a more deliberate security framework.

Formalized communication in this risk area is already planned as part of the MUS enterprise risk management (ERM) process initiated by the Board of Regents. Information security has been identified as a system-wide risk, and as part of the ERM process, the workgroup will have a reporting line to the Board of Regents through our MUS Risk and Compliance Leadership Council.

Lastly, the process described above will help OCHE determine what resources are needed across the system and/or at OCHE to support IT governance and information security across the MUS. OCHE will identify any additional resources needed by April 2023.

UNIVERSITY OF MONTANA

March 24, 2022

Angus Maciver
Legislative Audit Division
Room 160 State Capitol
P. O. Box 201705
Helena, MT 59620-1705

Dear Mr. Maciver:

On behalf of the University of Montana, I want to extend our appreciation to you and your staff for their work on the audit of information security and practices managed by the University of Montana and the Montana University System. We value the input of the legislative audit staff as we continue to develop our security program.

Again, thank you and your staff for their assistance and attentive efforts.

Sincerely,

Seth Bodnar
President
University of Montana

c: C. Christian, Commissioner of Higher Education

Bodlet109
SB/kw

University of Montana
Response to Information Systems Audit Recommendation

Recommendation #2

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

The University concurs. Role descriptions for key positions overseeing the security program have not changed since they were revised and communicated to the incumbents in 2020. The University notes that the role descriptions reviewed during this audit were formatted differently and will ensure that the same template is used for all role descriptions. This corrective action plan will be implemented by June 30, 2022.

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.

The University concurs. The University will complete a comprehensive IT risk assessment and implement strategic initiatives with an eye toward maturing the security program and increasing security awareness. This corrective action plan will be implement by June 30, 2023.

MONTANA
STATE UNIVERSITY

March 24, 2022

Mr. Angus Maciver
Legislative Auditor
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705

Dear Mr. Maciver:

Montana State University would like to thank the Legislative Audit Division for their time in auditing information security in the Montana University System. We believe this audit was productive and helpful in ensuring that information security related processes are operating as intended. We look forward to working with you again during the next audit.

Sincerely,

Waded Cruzado
President

WC/cr

Office of the President
216 Montana Hall
P.O. Box 172420
Bozeman, MT 59717-2420
www.montana.edu

Tel 406-994-2341
Fax 406-994-1893

Mountains & Minds

MONTANA STATE UNIVERSITY
Response to Legislative Audit Division Recommendation
Information Security in the Montana University System

Recommendation #3

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

Response:

Montana State University concurs with this recommendation. Our Corrective Action Plan includes the following:

- The more formal adoption of an information security related framework to further assess existing controls and procedures and further understand and address risk.
- The more formal assessment of risk specifically related to the Gramm-Leach Bliley Act.
- The documentation of how existing controls address risks identified in the Gramm-Leach Bliley Act more formal risk assessment.

Montana State University plans to complete this Corrective Action Plan by April 1, 2023.