A Report
to the
Montana
Legislature

Information Systems Audit

eGovernment Series: Security Consolidation

Department of Administration

June 2022

Legislative Audit
Division

20DP-04

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 Hallinan
Hunter McClure

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

June 2022

The Legislative Audit Committee
of the Montana State Legislature:

This is the first report of our information systems audit eGovernment series. This series of reports is focused on the State Information Technology Services Division's (SITSD) statewide IT strategic plans that relate to eGovernment. It provides the Legislature information about the Department of Administration's role in providing IT services to citizens and state agencies.

This first report focuses on the security consolidation initiative managed by SITSD within the Department of Administration. This report includes a recommendation for improving security consolidation planning at the Department of Administration. A written response from the Department of Administration is included at the end of the report.

We wish to express our appreciation to Department of Administration's personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Administration	Misty Ann Giles, Director
	Kevin Gilbertson, Chief Information Officer, SITSD
	Andy Hanks, Chief Information Security Officer, SITSD

Montana Legislative Audit Division

eGovernment Series: Security Consolidation

Department of Administration

Background

The Department of Administration is responsible for carrying out the planning and program responsibilities for IT in state government. With a new administration taking office in January 2021, the statewide strategy on IT has changed.

To ensure timely recommendations on new initiatives and services we will issue multiple focused reports. The focus of this report is on the consolidation of IT and security staff under the State Information Technology Services Division (SITSD) within the Department of Administration.

Agency:
Department of Administration

Director:
Misty Ann Giles

Program:
State Information Technology Services Division

IT consolidation and optimization has been a top 10 priority for chief information officers across the U.S. since 2007. Part of the new MT Executive Administration's IT strategy is to consolidate State security operations under the state chief information security officer. Consolidation efforts have occurred, and other agencies are apprehensive about the path moving forward. A statewide consolidation strategy needs to be developed to communicate changes, create and track consolidation goals, and ensure agency buy-in and consolidation success.

KEY FINDINGS:

SITSD does not have a statewide strategy for security consolidation. SITSD consolidated Department of Labor and Industry IT services and security roles in January 2022. This consolidation prompted confusion at agencies on what security consolidation entailed. SITSD needs a statewide strategy for security consolidation that includes a communication and change management plan.

RECOMMENDATIONS:

In this report, we issued the following recommendation:

To the department: 1
To the legislature: 0

Recommendation #1 (page 14):
Governance, risk assessment, and planning
SITSD needs to develop a statewide security consolidation strategy that clearly defines communication and change management, key performance indicators, and roles and responsibilities between agencies and SITSD.

Department response: Concur

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

Chapter I – Introduction, Scope, and Objectives

Introduction

Electronic government service (eGovernment) is a set of Internet applications that provides a specific service to a citizen, business, or other governmental entity. The goal of an eGovernment service is to provide a complete start-to-finish solution to the customer whenever possible. When online services are implemented in this fashion, both the state and the customer should gain efficiencies.

The concept of eGovernment has been around for over 20 years. As government services have grown to primarily rely on technology, the term has become synonymous with online services provided by a government enterprise. According to the State Information Technology Services Division (SITSD) 62 different state agencies, organizations, universities, and local governments offer more than 400 online services to benefit Montana's citizens.

Within Montana, every agency has a role in deciding what eGovernment will look like based on its operations and mission to serve the public. However, SITSD within the Department of Administration (department) also plays an essential role in delivering eGovernment services. SITSD's role in eGovernment is reflected in their mission: to provide standardized, strategic, secure, and state-of-the-art information technology to advance the efficiency and delivery of government service. With that distinction, SITSD is not an eGovernment manager and servicer but rather a government manager and servicer. SITSD has positioned itself as a service organization and provides varying services to three main groups: citizens, state agencies, and the Legislature.

In order to accommodate and provide this wide range of government services SITSD is intending to coordinate digital services across the State of Montana. To make this change SITSD is undergoing a digital services transformation and wants to shift how citizens and agencies digitally interact and access services from the State of Montana.

eGovernment Landscape Changes in the Past Three Years

Since 2001, the State of Montana had contracted with a third-party vendor to provide key electronic services:

1. A payment portal for online services,
2. Single sign on service, and
3. eGovernment application development as part of a "self-funding" model which includes work in exchange for a share of transaction fees applied to payments.

In 2019, the state contract with the third-party vendor for eGovernment services was soon to expire. Due to this, the state CIO appointed an eGovernment workgroup to research a new model focusing on identifying how to transition into a new contract. The workgroup made recommendations for a new eGovernment model that covered payment services and processing policy, supporting legacy applications, development of new services, single sign-on services, and collection and use of transaction

fees. The most significant changes in the new model come in the form of separate vendors for single sign-on service, application development, and payment processing. At the same time, SITSD would manage the transaction fee from payment processing. SITSD would also play a more prominent role in maintaining the previous vendor's applications.

Change in Administration Leads to a Change in Audit Approach

Initially, we identified risks with the decisions to restructure eGovernment that related to the following:

- The governance structure and transparency of decision-making within SITSD,
- Sustainability of the new funding model, and
- Compliance procedures and security controls over eGovernment applications.

In 2021, a new executive administration took over governing responsibilities, and since that time, SITSD has focused on improving the structure of online services through the state strategic plan. These initiatives significantly change the landscape of eGovernment, such as restructuring security responsibilities and the funding model. Therefore, we updated our approach to review this administration's new activities. We aligned our new objectives with SITSD's proposed statewide IT strategic goals to improve eGovernment. While the new administration shifted the eGovernment landscape, there is still uncertainty and risk over guidance on security for eGovernment applications, transaction fee uses, transparency over decision-making, collaboration efforts between agencies and SITSD, and how SITSD would report information to agencies and the Legislature.

With the implementation of these initiatives over the 21-22 biennium and these risks still in mind, we needed to approach the audit differently. Contained within the *Government Auditing Standards* our office follows is the concept of prospective analysis. Prospective analysis involves providing analysis or conclusions about events that may occur in the future, along with possible actions that the auditee may take in response. With that in mind, this audit is forward-facing, and will focus on activities that SITSD plans on conducting over the next two years.

Multiple Audit Reports Will Be Produced to Ensure Timely Recommendations

Our series of work on eGovernment will involve five objectives, focusing on a strategic goal area. Due to audit areas being tied to SITSD strategic goals, fieldwork will be prioritized based on SITSD's timelines. There will be multiple reports to promptly issue recommendations so that SITSD can incorporate findings into its strategy. SITSD strategic areas for review include:

- Security Consolidation
- IT Asset Management
- IT Innovation Funding
- IT Reporting
- Statewide IT Strategy and Performance Measurement

Audit Scope and Objectives

According to SITSD's statewide strategic IT plan, there will be an effort to consolidate security and IT support roles under SITSD. There remain risks and uncertainty surrounding responsibilities in maintaining agency application security, a security review of newly acquired eGovernment applications, and the impact security consolidation has on eGovernment services. The focus of this report will be on SITSD's security consolidation efforts. Consequently, we developed the following objective for this examination.

- Determine if SITSD's security consolidation and management will improve Montana's security posture.

The scope of the audit included identifying relevant state law regarding SITSD's authority over state IT and overall security responsibilities and researching IT industry frameworks on governance and IT service delivery. We also interviewed SITSD and agency chief information officers on the potential impact of security consolidation and discussed security consolidation initiatives with other states.

Audit Methodologies

Methodologies conducted for the above objective are summarized below:

- Identify new roles and responsibilities of SITSD and consolidated agencies.
- Identify relevant state law and policy regarding SITSD security governance responsibility and ability to reallocate security resources.
- Research and interview other states and national associations on security consolidation approaches.
- Interview SITSD employees on security consolidation plans and what approach is being undertaken.
- Interview other agency chief information officers to determine what they expect from security consolidation and how it should unfold.

We also reviewed industry standards for governance and IT service delivery to determine how they can be applied to Montana's security consolidation efforts. Industry standards include:

- Control Objectives for Information and Technology (COBIT): Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks.
- Information Technology Infrastructure Library (ITIL): A set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of business. This guidance helps organizations address new service management challenges and utilize technology efficiently.

Chapter II – Security Consolidation

Introduction

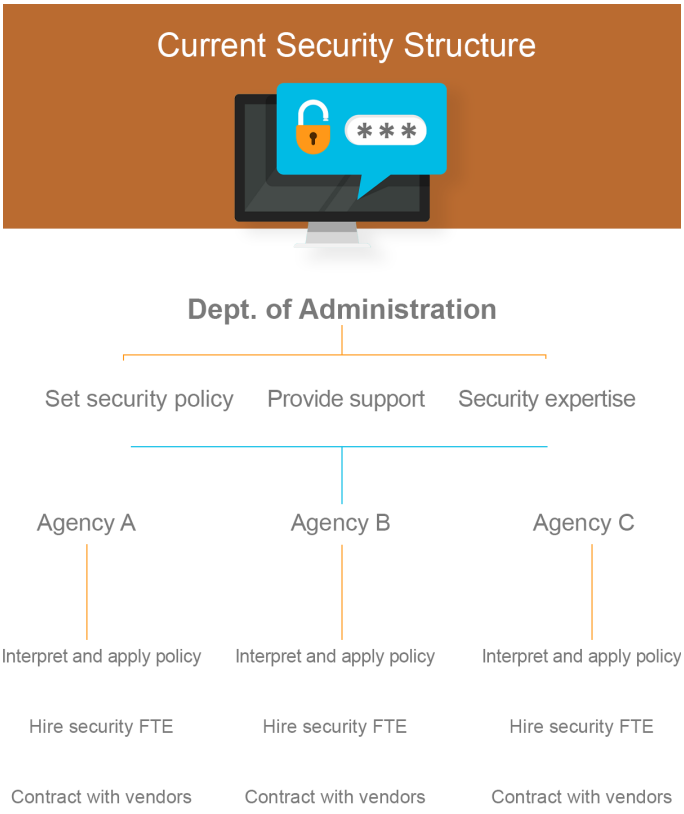
Before each legislative session, SITSD must produce a statewide strategic IT plan. Part of the current plan is to ensure that citizens' data is protected along with the state's information assets. This includes the goal of consolidating state security operations under the state chief information security officer (CISO). Security consolidation is an enormous undertaking. One that involves moving personnel from one organization to another, new roles and responsibilities for organizations involved, and changes to agency budgets. Without a proper strategy in place, there can be severe impacts on the state's security posture.

While consolidation carries risks, most state chief information officers (CIOs) agree that a centralized security structure helps put CISOs in a better position to improve agility, effectiveness, and efficiencies.

Montana's Current Security Structure vs Consolidation

As it stands now, the department and SITSD direct IT policy and use their security expertise to provide support to agencies. Each agency has their own security program where they interpret and follow state IT policy, hire security personnel, and contract with vendors where appropriate. Figure 1 below shows this current relationship.

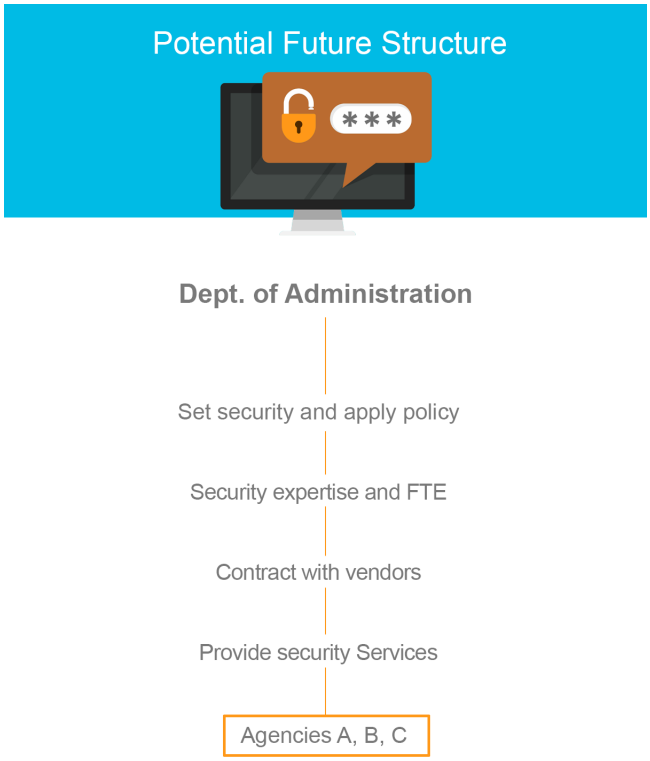
Figure 1
Current Security Structure



Source: Compiled by Legislative Audit Division staff.

In consolidation, individual security programs are rolled together into one security program. A later portion of this chapter discusses the benefits of consolidation, but a typical centralized structure could look like Figure 2 below.

Figure 2
Potential Future Security Structure



Source: Compiled by Legislative Audit Division staff.

Security Consolidation in State Government Can Happen in More Than One Way

Title 2, Chapter 17, Part 5 of the Montana Code Annotated describes the state's IT requirements and makes the Department of Administration (department) responsible for carrying out the planning and program responsibilities for IT in state government. Section 2-17-512, MCA, lists multiple responsibilities, including the need to:

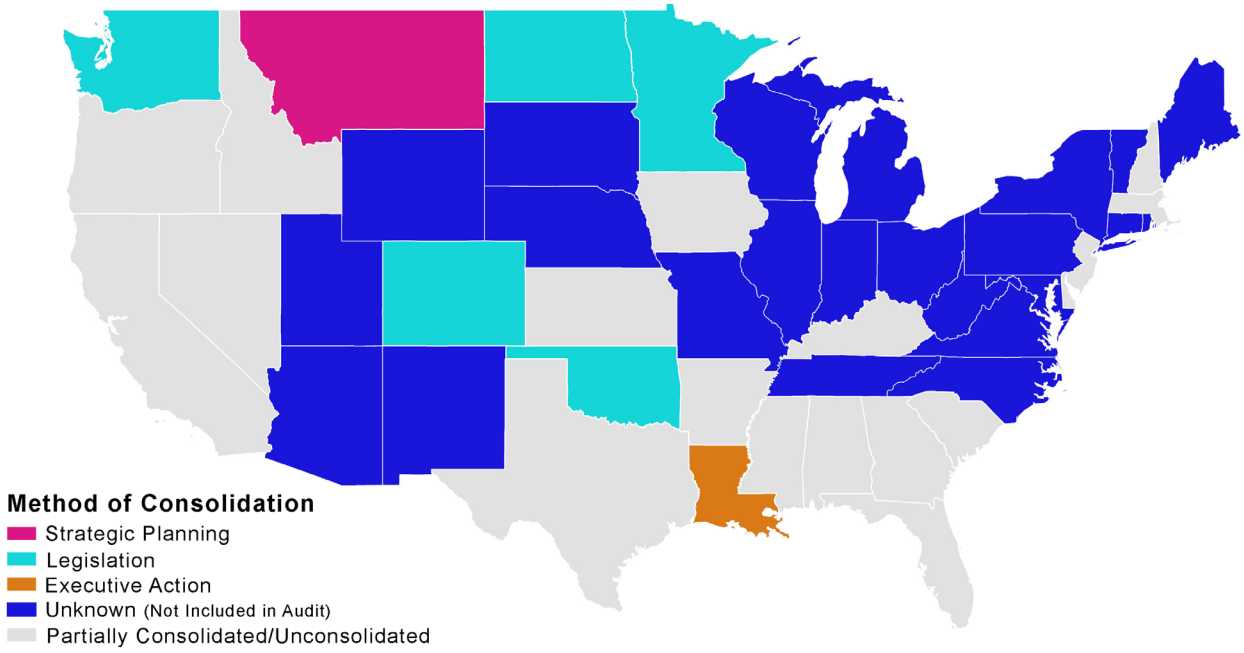
- Promote, coordinate, and approve the development and sharing of shared information technology application software, management systems, and information that provide similar functions for multiple state agencies.
- Cooperate with the office of economic development to promote economic development initiatives based on information technology.
- Establish and enforce a state strategic information technology plan.
- Review the use of information technology resources for all state agencies.

Through these responsibilities, the department has the power to coordinate and consolidate IT resources across the state.

Through research and discussions with the National Association of Chief Information Officers (NASCIO), we identified states that have undergone security consolidation efforts. Over the last 15 years, security consolidation has been a priority for CIOs across the U.S. Consolidation has taken a different form in these states, but they all have a centralized IT implementing security practices across the enterprise. The following figure shows some of the states that have been consolidated over the past 14 years highlighted in the NASCIO discussion.

Figure 3

States That Have Undergone Consolidation



Source: Compiled by Legislative Audit Division staff.

National Guidance for Security Consolidation

In 2020, NASCIO produced a Cybersecurity Study that reflects the insights on cybersecurity from all 50 states. One fundamental takeaway is that a centralized security structure helps CISOs position cybersecurity in a way that improves agility, effectiveness, and efficiencies. Our interview with NASCIO also highlighted national guidance and lessons learned from some of the recent efforts to consolidate security.

- **Best Fit Approach:** They emphasized the need to use a blended framework approach where an organization pulls best practices from multiple frameworks to implement security consolidation.
- **Formal Agreements:** Cybersecurity needs to be considered in agreements between centralized IT and agencies focusing on risk mitigation. Agencies are not wholly unique from a security perspective. A standard Memorandum of Understanding (MOU) or Service Level Agreement via service catalog can help streamline the consolidation process.
- **Communication:** NASCIO stressed the importance of how security consolidation is a PR campaign for agency management and the individuals personally affected by consolidation. Consolidation has many moving parts, and one aspect that must not be

forgotten is the people. Centralized IT needs to do everything it can to listen and help people throughout the process and quell any fears they may have.

There is a trend of security consolidation across the United States. Security consolidation in Montana can increase the State's security posture while also producing additional benefits such as less competition for security personnel hiring between agencies, improved support for agencies, and cost avoidance. However, a statewide strategy needs to be developed. SITSD has not created this strategy, nor ways to measure the value and benefit of security consolidation.

Security Consolidation Has Occurred, but No Statewide Strategy Is in Place

In January 2022, the Department of Labor and Industry's (DLI) desktop management, help desk support, system administration, and security roles were consolidated under SITSD. SITSD did not intend for this to be a consolidation strategy that will be used for all other agencies. While this may not have been part of the overall consolidation plan, the communication and perception by agency staff has been that this is the first step, or pilot, in the consolidation effort.

The process for DLI's consolidation started with an assessment. In June 2021, DLI, SITSD, and a third-party vendor conducted an organization and systems assessment of DLI's Technology Services Division. SITSD indicated an assessment was necessary due to concerns with staffing impacts on security and services. The assessment was meant to determine the best path forward for DLI IT operations. Recommendations stemming from this assessment included centralizing of DLI IT personnel in key areas under SITSD. This was conducted via an MOU between DLI and SITSD and a budget change request to the Governor's Office of Budget and Program Planning.

While a final statewide consolidation strategy was not developed during our audit, a draft was available at the end of fieldwork. The plan for DLI's transition may not represent the plan for other agencies, but there are lessons to learn in communication and strategy for future consolidation efforts. SITSD needs to develop a concise consolidation strategy with measurable goals. This will help address any negative perceptions that agencies may have about consolidation and promote the benefits that should be expected.

Communication, Roles, Responsibilities, and Time Frames Need to Be Identified

We also interviewed agency CIOs to get their perspective on consolidation. Agencies have been confused about what was happening with consolidation. Official notification of the DLI's consolidation was sent out in January 2022, but agencies have not received any other official guidance or information. SITSD indicated it had to delay the rollout of consolidation due to personnel constraints and the Governor's focus on a telework and office space study.

There was clear skepticism from our conversations with agency CIOs about how successful security consolidation will be. However, they all discussed the same concepts they would like to see for consolidation to move forward positively.

1. Communication Plan and definition of which specific areas will be centralized in security consolidation.

2. MOU or Service Level Agreement in place that defines SITSD's and agency's roles and responsibilities.
3. Defined goals and cost savings.

Overall, the agencies felt security consolidation is the right move. However, there is a perception of consolidation starting with DLI and a lack of communication from SITSD has caused confusion.

Various Frameworks Offer Blended Guidance on Consolidation

Various frameworks exist to guide IT organizations through transitions such as this. We chose to look at one that focuses on management practices and another on service management due to SITSD's role in state government.

IT Management Practices from the Control Objectives for Information and Technology (COBIT)

SITSD could use the following specific objectives from COBIT to manage security consolidation's strategy from a governance perspective.

- **Consistent Management Approach**

  SITSD needs to evaluate their governance structure and determine if changes need to be made to accommodate security consolidation. They need to define and communicate roles and responsibilities for enterprise IT including authority levels, responsibilities, and accountability. A consideration that needs to be made when determining the management approach is how do consolidated agency CIOs play into decision-making.

- **Strategy**

  Security consolidation needs to be clearly connected to an overarching strategy. An assessment of the current performance of IT (GAP Analysis) needs to occur to develop an understanding of current capabilities with metrics identified and tracked to define success.

- **Human Resources**

  SITSD needs to provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation, and development of human resources. They need to consider the financial impact of taking on more FTE at SITSD and how that changes all agencies' future budget requests to legislators.

- **Relationships**

  Managing relationships with agencies formally and transparently will ensure mutual trust. Roles and responsibilities need to be defined, assigned, and communicated between SITSD and agencies. Additionally, SITSD needs to continually improve and evolve IT-enabled services and service delivery to the enterprise to align with changing enterprise objectives and technology.

- **Quality**

  Quality requirements surrounding security consolidation should be defined and communicated focusing on processes and procedures. Definition of metrics of success and a focus on continuous improvement will ensure a successful rollout.

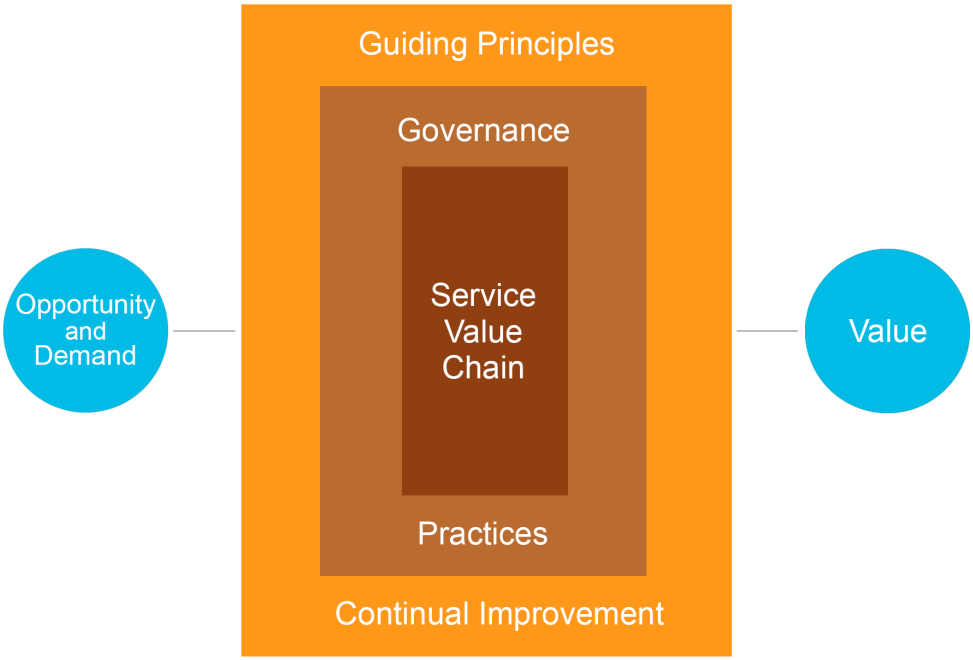
- **Security**
  SITSD needs to consider how taking over agency security operations impacts the current system. Similar to IT management, the placement and responsibilities of security personnel need to be considered. This can be done in various ways, ranging from agencies completely relying on SITSD for security, to a SITSD liaison at each agency to help guide them on security matters.

IT Service Management Practices From the Information Technology Infrastructure Library (ITIL)

Value is co-created through collaboration between providers (SITSD) and consumers (agencies). Communication between these entities is vital to maintaining services while undergoing organizational changes. SITSD needs to establish/enhance interactive relationships with agencies to ensure consolidation success. Figures 4 and 5 highlight ITIL concepts that can help SITSD form their consolidation strategy.

The ITIL service value chain describes how all the components and activities of the organization work together as a system to enable value creation. Figure 4 shows this system.

Figure 4
Service Value Chain



Source: Reproduced by Legislative Audit Division staff from the Information Technology Infrastructure Library.

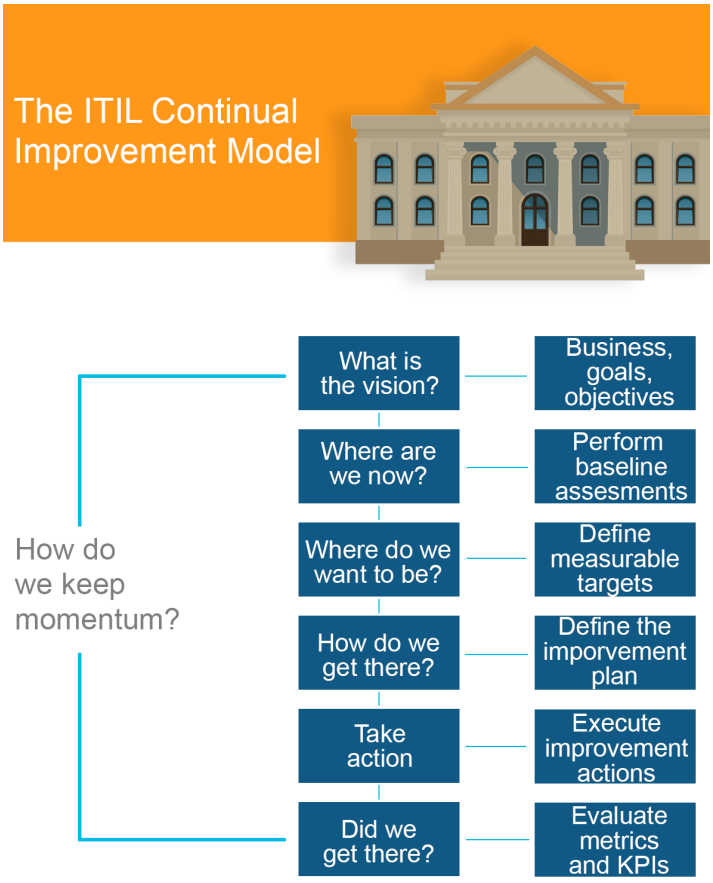
Within the consolidation context, there is demand for security services from agencies. SITSD needs to implement a proper governance system to ensure value is created for everyone. Agencies will receive security services and expertise and SITSD will be able to ensure state enterprise is secure. This approach stresses guiding principles such as frequent communication and coordination across the enterprise while identifying how to continually improve services. However, there are still challenges that can impede this co-created value.

Organizational silos, such as the agency structure within state government, can be one of the biggest challenges in creating value. In the past, SITSD and agency communication has been stifled. There needs to be an exchange of information with agencies at key points in the consolidation process to remove these silos. If successful, the entire State enterprise benefits by having access to information and specialized security expertise.

Establishing the Service Value System is important, but continual improvement needs to be implemented to maximize the effectiveness of services. The ITIL Continual Improvement Model found below provides a high-level overview of how organizations can keep continual improvement in mind. It is SITSD's responsibility to ask themselves and agencies key questions about consolidation in order to create and evaluate metrics and key performance indicators. This model can help ensure SITSD and agencies continually work together to co-create value.

Figure 5

Continual Improvement



Source: Reproduced by Legislative Audit Division staff from the Information Technology Infrastructure Library.

The Service Value System and Continual Improvement model help organizations improve existing processes. However, SITSD and agencies have yet to undergo organizational change to implement security consolidation. The table shows the activities they must undergo and describes the purpose of those activities.

Table 1
Organization Change Management Activities

Activity	Helps to Deliver
Creation of a sense of urgency	Clear and relevant objectives, willing participants
Stakeholder management	Strong and committed participants
Sponsor management	Strong and committed leadership
Communication	Willing and prepared participants
Empowerment	Prepared participants
Resistance management	Willing participants
Reinforcement	Continual improvement

Source: Reproduced by Legislative Audit Division staff from the Information Technology Infrastructure Library.

To achieve successful organizational change, SITSD should communicate security consolidation in way that generates a sense of urgency for agencies and stresses the importance of the change. At the time of the audit, SITSD did not know which agencies were going to be consolidated and was not at a point to start communicating with them. In future communications, SITSD should identify all stakeholders and sponsors of consolidation in order to know who they should be communicating with and what best suits their needs. Part of this process involves ensuring those part of consolidation feel empowered. This is done by providing proper equipment, training, and time to undergo the change. SITSD may also encounter resistance to consolidation and should dedicate time to identifying and understanding why there is resistance. Finally, SITSD needs to reinforce the importance of consolidation via continual improvement and communication.

During our audit, SITSD was developing an initial consolidation plan, but was not able to show how these concepts were going to be included. SITSD needs to develop a consolidation plan that incorporates a management framework and IT service delivery framework into their security consolidation strategy. SITSD should also ensure measurable goals are set and tracked throughout consolidation. While undertaking these activities, SITSD should consider cultural differences at each agency and hold themselves accountable. Ultimately, it is important for SITSD to focus on communication about the process with stakeholders such as agencies and the legislature in order to ensure transparency.

Measurable Goals and Key Performance Indicators Can Help Ensure Success

Security consolidation will change how SITSD provides services, and they need to ensure that these changes are implemented effectively and are measured. In our interview with NASCIO, several goals were identified that other states have used to measure consolidation success. NASCIO provided examples of cost savings for consolidating IT services as a whole and not just security. By combining executive cabinet agencies such as the Offices of Computing Services, Information Services, Telecommunications Management, and Information Technology, Louisiana announced that the state saved about $75 million in the first year of consolidation. Oklahoma consolidated IT infrastructure services such as baseline security, e-mail services, virus protection, desktop management, and

commercial software license management and estimated that consolidation would save approximately $77 million over six years. It is too soon to estimate how much money could be saved in Montana, but SITSD can consider other types of goals, such as enhancing security, when forming their strategy to measure success.

- **Improve Security Posture/Cost Avoidance**
  - » Strengthen IT security with the adoption of standard controls and tools to reduce impact and cost of cyber incidents.
  - » Reduce diversity and complexity of IT environment.
  - » Improve support for legacy systems by utilizing the best IT talent on critical enterprise systems and infrastructure.
  - » Create knowledge transfer by training security to provide services to multiple agencies.
- **Potential Cost Savings**
  - » Create economies of scale by renegotiating vendor contracts and sharing software licensing amongst agencies.
  - » Reduce operational costs with consolidation of common IT services for end users.
  - » Promote enterprise integration and applications.
  - » Centralize infrastructure maintenance and upgrades.
  - » Less competition between SITSD and agencies to hire security professionals.

In some instances, the goal of consolidating security is not to reduce costs but avoid them. Improving security posture via consolidation will decrease the likelihood of security breaches and avoid costs associated with them. Whichever metrics SITSD chooses, they need to align the goal of security consolidation with the needs of the stakeholders. SITSD has taken the stance that consolidation is about cost avoidance rather than cost reduction but has not developed the metrics to understand what costs are being avoided and what value security consolidation provides the State. Therefore, metrics should be set up to identify if cost avoidance is achieved. Even though the intention of consolidation is not to reduce cost, it is still important to be transparent about costs and expectations as well.

DLI Consolidation and Other States Lessons Can Help Shape State Strategy

Even though DLI's security consolidation was not part of SITSD's overall state consolidation strategy, lessons can be learned for future consolidations.

During our interviews with agency CIOs, we were apprehensive because they had not seen any official communication from SITSD on what security consolidation meant. They expressed the need for a:

- Change management plan,
- Assurance that the level of service an agency receives would not be diminished,
- Information on moving employees from union to non-union organizations,
- Timeline for consolidation and,
- Cost allocations for agencies.

SITSD can incorporate these agency needs into their statewide security consolidation strategy to ensure it is successful and they receive agency buy-in.

SITSD can also learn from other states. In 2019, the Minnesota Office of the Legislative Auditor evaluated the state's consolidation efforts. Key findings include divided opinions from state agencies about consolidation, concern about the level of service from consolidation and security costs, and confusion about responsibilities between Office of Minnesota Information Technology Services (MNIT) and agencies. MNIT has not provided Legislature and state agencies with sufficient information on its performance. This report showed the possible effects of moving forward with consolidation without a plan to address these types of risks and Montana can learn from these mistakes when forming a consolidation strategy.

The main takeaways SITSD can use when forming their strategy are identifying and personalizing IT management and service delivery frameworks to fit Montana's needs, creating and tracking key performance metrics to measure success, and, most importantly, remembering the people. Consistent communication can help agencies and individuals feel secure in what the future may hold and ultimately help ensure a successful consolidation.

RECOMMENDATION #1

We recommend that the State Information Technology Services Division (SITSD) reference appropriate frameworks and create a statewide security consolidation strategy prior to consolidating other agencies that includes:

A. *Communication and change management plan,*

B. *Key performance indicators and measurable goals for success, and*

C. *Newly identified roles and responsibilities between agencies and SITSD via standard Memorandum of Understanding.*

Security Consolidation Strategy Starts to Be Defined and Upcoming Series Reports

At the end of our fieldwork, we sat down with SITSD to discuss the audit findings. At this meeting SITSD was able to provide us a draft strategy for security consolidation. Upon review, we found that this draft strategy had elements of the criteria we gathered but no specific details. The criteria we gathered can help bolster the draft strategy and help ensure a proper security consolidation strategy is implemented.

SITSD still has work in other strategic areas including IT asset management, IT innovation funding, IT reporting, and statewide IT strategy and performance measurement. We anticipate that the next report in the series will be on IT asset management, in the fall of 2022. However, this timeline is depending on SITSD's plans and can change.

Department of Administration

Department Response

MONTANA DEPARTMENT OF ADMINISTRATION

Director's Office
Greg Gianforte, Governor
Misty Ann Giles, Director

June 6, 2022

RECEIVED
June 6, 2022
LEGISLATIVE AUDIT DIV.

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

RE: Information System Audit Report

Dear Legislative Auditor Maciver:

Upon review of the Information System Audit report of the security consolidation process, the Department of Administration concurs with the Legislative Audit Division's recommendations. At this time, the State Information Technology Services Division (SITSD) is still developing a comprehensive plan to centralize cybersecurity that will include organizational change management, key performance indicators, and a standard Memorandum of Understanding (MOU). The following provides a brief overview of the plan and some initial considerations.

The primary objective of centralizing cybersecurity is to enhance state government's overall cybersecurity posture. Centralizing cybersecurity under the State CISO will unify the State's cyber resources under a single strategy and governance structure to efficiently and effectively allocate resources based on risks, increasing consistency and quality of security services through standardization and automation, and improve transparency and return on investment of the cybersecurity budget.

The current decentralized cybersecurity model is wholly insufficient to protect citizen's data in today's sophisticated threat environment, cybersecurity job market, and budget allocated for cybersecurity. Cyber threats actors utilize advanced tactics, techniques, and procedures to infiltrate networks, establish persistence, and exfiltrate sensitive data. It takes an average of 287 days to identify and contain cyber threat actors on your network. As all state agencies share the same network, any attack on one agency

125 North Roberts, Rm 155, Mitchell Building
P.O. Box 200101
Helena, MT 59620-0101
406-444-2032
doadirector@mt.gov
doa.mt.gov

poses risks to all other agencies; we are only as strong as the agency with the weakest cybersecurity posture on our network. The high demand – low supply cybersecurity job market makes it very difficult for the public sector to compete with the private sector for skilled and diverse cybersecurity talent. In our current environment, agencies compete for limited cybersecurity resources, sometimes poach cybersecurity employees from other agencies, or they simply cannot fill their cybersecurity positions. Most agencies have less than one employee dedicated to cybersecurity and few agencies have the resources necessary to properly invest in cybersecurity employee development. Agency investments in the people, processes, and technology supporting their cybersecurity vary greatly from one agency to the next and are often buried in other IT and non-IT budget line items. This makes it difficult to identify the true spend on cybersecurity statewide and nearly impossible to measure return on investment in cybersecurity. The lack of or uneven investment of cybersecurity across all agencies creates an imbalance that increases risks for all agencies and proliferates spend on redundant functions.

Centralizing cybersecurity was identified as a strategic objective during the State IT Strategic Conference in August 2021. The State CISO started developing a high-level plan in April 2022 to consolidate cybersecurity resources in Executive Branch agencies without elected officials. Since then, additional stakeholders, including agency leaders and employees, have provided input into the draft plan. As stated within the audit report, SITSD's centralizing cybersecurity plan is still in a draft stage, so it does not yet include all the recommendations that are included within the report. We are currently drafting an MOU template for centralizing cybersecurity. This MOU will be shared with agencies for their input before being finalized. We are also scheduling meetings for the State CIO and State CISO to meet with each agency Director, Deputy Director, and CIO to review the draft plan and gain an understanding of their cybersecurity needs and resources.

The centralizing cybersecurity project is divided into four phases: (1) Planning, (2) Transition, (3) Transformation, and (4) Steady State. Planning is about preparing for the consolidation process. During the planning phase we identify guiding principles, critical success factors, key stakeholders, and communication strategies. Transition is about minimizing change and learning more about agency security needs and employee training needs. During the transition phase, employees organizationally move into a new agency-focused bureau under the CISO, they still support their agencies using their security processes, we learn about agency security processes to identify best practices, we participate in team activities, and we build a new shared culture together. Transformation is about implementing change. During transformation, we standardize best practices across agencies, implement automation and reporting, and provide training to employees. Steady State is the end goal. During Steady State, we realize the benefits of centralizing cybersecurity, we measure and report risk and performance metrics, and we continuously improve.

Some of the guiding principles of this effort include open and transparent communication, employee focus, and agency security posture. Open and transparent communication is achieved by communicating what we know when we know it and by listening, learning, and adapting. Employee focus is achieved by consideration of the employee's perspectives, relationships, and job security; and by clearly communicating expectations. Agency security postures will be enhanced by this effort, benefiting from institutional knowledge, subject matter expertise, and more resilient security resource pools.

We understand that communication is critical to the success of this project. We will continue to discuss our planning in every agency meeting, CIO roundtable, and cabinet meeting; but we will also start communicating in dedicated consolidation meetings with stakeholders going forward to alleviate the concerns expressed in this report. We are taking time to plan this consolidation because we believe it is better to get it right than to do it fast. The State has never centralized an enterprise function in state government before; we will make mistakes, we will learn from those mistakes, and we will improve our process. Furthermore, transition from one phase to the next during this project will not occur based on arbitrary target dates. We will only move to the next phase when all the objectives in the current phase successfully complete and we incorporate any lessons learned into the next phase.

In conclusion, this consolidation effort is focused on ensuring the comprehensiveness of the State's information security program, creating benefits for state government, agencies, employees, and citizens. SITSD thanks the Legislative Audit Division for their hard work and thorough research documented in this report and will incorporate their recommendations in our planning process.

Sincerely,

Misty Ann Giles
Director, Department of Administration

c: Kevin Gilbertson, Chief Information Officer, SITSD
Andy Hanks, Chief Information Security Officer, SITSD