



A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION TECHNOLOGY AUDIT

*Vendor-First Approach to
Agency IT Services: DLI
Test Case for Controlling
Shared Services*

*Department of Labor and Industry
Department of Administration*

AUGUST 2024

LEGISLATIVE AUDIT
DIVISION

23DP-03

INFORMATION TECHNOLOGY AUDITS

Information Technology (IT) audits conducted by the Legislative Audit Division are designed to assess controls in an IT environment. IT 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 IT 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 IT audit staff hold degrees in disciplines appropriate to the audit process.

IT audits are performed as stand-alone audits of IT 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.

LEGISLATIVE AUDIT COMMITTEE

REPRESENTATIVES

LYN HELLEGAARD
Lyn.Hellegaard@legmt.gov

SJ HOWELL

SJ.Howell@legmt.gov

EMMA KERR-CARPENTER
Emma.KC@legmt.gov

FIONA NAVE

Fiona.Nave@legmt.gov

JERRY SCHILLINGER

Jerry.Schillinger@legmt.gov

LAURA SMITH, VICE CHAIR
Laura.Smith@legmt.gov

SENATORS

JASON ELLSWORTH, CHAIR
Jason.Ellsworth@legmt.gov

PAT FLOWERS

Pat.Flowers@legmt.gov

CHRIS FRIEDEL

Chris.Friedel@legmt.gov

DENISE HAYMAN

Denise.Hayman@legmt.gov

KATHY KELKER

Kathy.Kelker@legmt.gov

FORREST MANDEVILLE

Forrest.Mandeville@legmt.gov

MEMBERS SERVE UNTIL A
MEMBER'S LEGISLATIVE TERM
OF OFFICE ENDS OR UNTIL A
SUCCESSOR IS APPOINTED,
WHICHEVER OCCURS FIRST.

§5-13-202(2), MCA

FRAUD HOTLINE
(STATEWIDE)
1-800-222-4446
(IN HELENA)
444-4446
LADHotline@legmt.gov
www.montanafraud.gov

AUDIT STAFF

HUNTER McCLURE

MIKI CESTNIK

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

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Kenneth E. Varns, Legal Counsel



Deputy Legislative Auditors:
Cindy Jorgenson
William Soller
Miki Cestnik

August 2024

The Legislative Audit Committee
of the Montana State Legislature:

We are pleased to present our information technology audit of the shared IT control structure managed by both the Department of Labor and Industry (DLI) and the State Information Technology Services Division (SITSD) at the Department of Administration (DOA). As agencies bring in more IT services from other entities, management of IT controls shifts among the entities and a greater responsibility is now shared between them. This audit represents a collaboration and understanding of responsibilities between DLI, SITSD, and their vendors.

This report provides the Legislature information about DLI's ability to coordinate with business partners such as SITSD while implementing large-scale changes such as IT service consolidation and new system implementation. This report includes recommendations for DLI to improve leadership accountability and vendor and organizational change management. A recommendation for SITSD is included to provide vendor management guidance and establish shared responsibilities with agencies. Written responses from both departments are included at the end of the report.

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

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

TABLE OF CONTENTS

Figures and Tables.....	ii
Appointed and Administrative Officials	iii
Report Summary	S-1
CHAPTER I – INTRODUCTION, SCOPE, AND OBJECTIVES	1
Introduction	1
Major IT Management and Consolidation Changes Over the Last Three Years	1
Audit Scope and Objectives	2
What We Did	3
User Survey	4
Criteria Used.....	4
CHAPTER II – DLI’S LEADERSHIP NEEDS TO BE ACCOUNTABLE FOR OVERALL IT CONTROL STRUCTURE.....	5
Significant Findings	5
Impact.....	6
Improvement Opportunity	6
CHAPTER III – DLI AND SITSD NEED TO DEFINE RESPONSIBILITIES IN THE SHARED IT CONTROL STRUCTURE.....	9
Significant Findings	9
Impact.....	10
Improvement Opportunity	11
CHAPTER IV – IMPROVED ORGANIZATIONAL CHANGE MANAGEMENT IS NEEDED FOR DLI TO TRANSFORM IT.....	13
Significant Findings	13
Impact.....	14
Improvement Opportunity	15
DEPARTMENT RESPONSES	
Department of Labor and Industry.....	A-1
Department of Administration	A-13

FIGURES AND TABLES

Figures

Figure 1	TSD Program and Services Before Consolidation	1
Figure 2	TSD and SITSD Program and Services After Consolidation	1
Figure 3	Inadequate Feedback Channels.....	11
Figure 4	User Familiarity with IT Modernization	15

Tables

Table 1	DLI Control Areas Summary	4
Table 2	Leadership Control Processes.....	5
Table 3	Shared Responsibility Control Processes.....	9
Table 4	Organizational Change Management Control Processes.....	13

APPOINTED AND ADMINISTRATIVE OFFICIALS

Department of Labor and Industry

Sarah Swanson, Commissioner, August 2023 - Present

Laurie Esau, Former Commissioner, January 2021 - June 2023

John Elizandro, Interim Commissioner, June 2023 - August 2023

Kim Warren, Technology Services Division Administrator, January 2022 - Present

Department of Administration

Misty Ann Giles, Director

Kevin Gilbertson, Chief Information Officer

Michele Snowberger, Deputy Chief Information Officer

Chris Santucci, Chief Information Security Officer

Michael Barbere, Enterprise Security Compliance Officer



MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION TECHNOLOGY AUDIT

Vendor-First Approach to Agency IT Services: DLI Test Case for Controlling Shared Services

DEPARTMENT OF LABOR AND INDUSTRY & DEPARTMENT OF ADMINISTRATION

A report to the Montana Legislature

BACKGROUND

The Department of Labor and Industry (DLI) manages the state’s unemployment program, which administers both unemployment insurance (UI) tax and benefits. DLI also provides services related to workforce development, occupational safety and health, and regulation of various industries within the state. The Technology Services Division (TSD) within DLI provides technical support for these programs. After turnover and various challenges within TSD, leadership identified opportunities for improvement in services and modernization efforts. In 2022, DLI and the State Information Technology Services Division (SITSD) consolidated IT service desk, system administration, and security operations to improve technology services and assist DLI in replacing old technology. In 2023, DLI implemented a new UI system, the Montana Unemployment Services Environment, which had a total cost of \$8 million.

The Department of Labor and Industry (DLI) recently made strides in enhancing services and upgrading technology but has struggled to implement its IT management program effectively. Unclear expectations and ownership, starting with executive management, have hindered the success of consolidation with the SITSD. Consequently, vital areas such as risk, security, IT service, and organizational change management lack oversight, jeopardizing the modernization of DLI’s systems and future collaboration with SITSD. Being one of the first agencies to consolidate IT services under SITSD, the success of DLI can impact statewide consolidation and security efforts and highlights the immediate need to address issues within DLI’s IT program.

KEY FINDINGS:

The figure below summarizes the nature and extent of the audit findings. Findings are categorized by priority that is based on impact and whether the agency has effective controls to mitigate the risk associated with the finding. Impact is the effect a risk could have on an agency’s system, security, business process, or operation. Each priority category contains the number of relevant findings in this report.

		Ability to control risk			
		High		Low	
Impact	Significant	Critical but Controlled		Highest Priority	1
	Moderate	No Major Concern		High Priority	3
	Minimal			Moderate Priority	

(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@legmt.gov

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

Text
(704) 430-3930

RECOMMENDATIONS:

In this report, we issued the following recommendations:

Priority from summary table: **Highest Priority**

RECOMMENDATION #1 (page 7):

Governance, risk assessment, and planning

The Department of Labor and Industry needs to follow statewide performance evaluation processes and ensure specific roles related to risk, vendor, and organizational change management are addressed in the Technology Services Division Administrator's occupation job standard.

Department response: Do Not Concur

Priority from summary table: **High Priority**

RECOMMENDATION #2 (page 11):

Procurement, contracting, and grants management

The Department of Labor and Industry needs to incorporate aspects of vendor management into existing policy and procedure, take accountability in the shared control structure, and work with the Department of Administration to develop a formalized shared responsibility model.

Department response: Do Not Concur

RECOMMENDATION #3 (page 12):

Governance, risk assessment, and planning

The Department of Administration, in conjunction with the State Procurement Bureau, needs to provide guidance and expectations to agencies on how to manage vendors. When providing services and sharing security responsibilities with agencies, the State Information Technology Services Division needs to establish clear roles and responsibilities.

Department response: Concur

RECOMMENDATION #4 (page 15):

Governance, risk assessment, and planning

The Department of Labor and Industry needs to strengthen its internal IT strategy process and ensure goals are communicated and measured.

Department response: Partially Concur

Chapter I – Introduction, Scope, and Objectives

Introduction

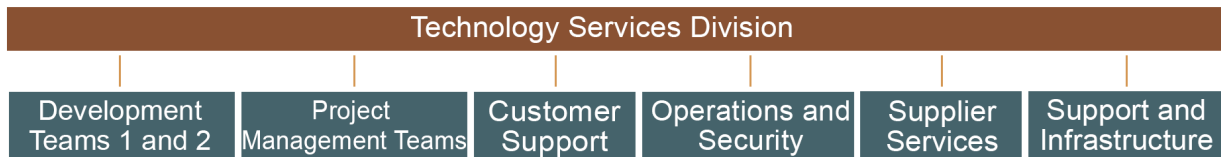
The Department of Labor and Industry (DLI) upholds labor laws, ensures worker safety, and supports business and employee relations through workforce services. The governor appoints the commissioner, who, through DLI’s five divisions, enforces state and federal labor standards, safety, and occupational health laws. DLI operates as part of a national employment, unemployment insurance, and job training system and helps workers obtain benefits if they are temporarily unemployed.

DLI’s Technology Services Division (TSD) provides technical support to the rest of the agency and works closely with the Department of Administration’s State Information Technology Services Division (SITSD).

Major IT Management and Consolidation Changes Over the Last Three Years

In 2021, a new executive administration took over governing responsibilities, and since that time, SITSD has focused on improving online services and IT structure through the state strategic plan. Due to concerns with staff turnover in security and services at TSD, DLI, and SITSD had a third-party vendor conduct an organization and systems assessment of TSD in June 2021. Recommendations stemming from this assessment included centralizing DLI IT personnel in key areas under SITSD. The graphic on the following page depicts TSD’s program and services before this consolidation.

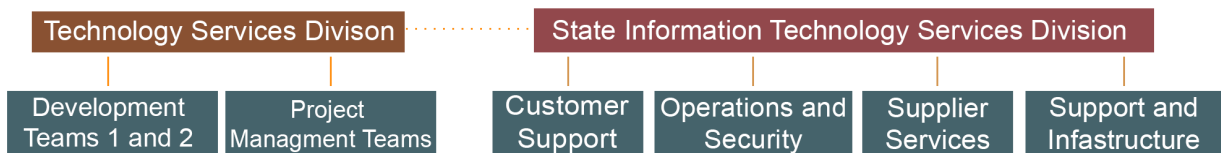
Figure 1
TSD Program and Services Before Consolidation



Source: Compiled by the Legislative Audit Division.

In January 2022, 15 FTE from DLI desktop management, help desk support, system administration, and security operations were consolidated under SITSD. The effect of this is reflected in the figure below with changes to TSD and SITSD program and services.

Figure 2
TSD and SITSD Program and Services After Consolidation



Source: Compiled by the Legislative Audit Division.

After the consolidation of DLI, SITSD started developing plans to consolidate the security operations of agencies. In June 2022, we finalized an audit titled: *eGovernment Series: Security Consolidation*. The report references various frameworks that offer guidance on consolidation and discusses consolidation steps taken thus far by SITSD. The lone recommendation from the report suggests that SITSD develop a statewide security consolidation strategy that clearly defines communication and change management, key performance indicators, and roles and responsibilities between agencies and SITSD. During the audit, we reviewed how DLI was consolidated via a memorandum of understanding. SITSD indicated the approach with DLI was not part of the larger statewide consolidation strategy; however, it stood as an example of more planning and coordination as DLI and SITSD moved into a shared control environment. Our follow-up to this audit identified that SITSD had developed a consolidation strategy for other agencies.

While a strategy and better planning are being used for other agencies based on the lessons learned from DLI in 2022, the effects of poor consolidation planning with DLI are still being felt two years later. Since 2022, DLI and SITSD have had undefined roles and responsibilities related to consolidation. Due to excluding DLI from the initial consolidation planning process, SITSD went back to reevaluate DLI's consolidation in August 2024 with plans for additional meetings later in the year. Additionally, in October 2023, DLI implemented the new unemployment insurance (UI) system, the Montana Unemployment Services Environment (MUSE). TSD has faced challenges adapting to these changes now that SITSD's previous role of only setting IT standards has shifted to more direct involvement in IT operations. A lack of planning during consolidation coupled with major IT changes has affected DLI areas like vendor management, risk assessment, security and organizational management, highlighting the need for leadership accountability.

Audit Scope and Objectives

The two audit objectives were to:

- ◆ Determine if DLI has implemented vendor management practices and safeguards the security of newly implemented IT application(s).
- ◆ Determine if DLI is managing organizational change, risk, and IT services to ensure success of multiple large IT initiatives.

Large-scale changes have brought more stakeholders into the supply chain and control structure at DLI, which has led to a greater need for IT governance. Now, a single vendor provides both systems for UI taxes and claims. With mission-critical services relying on these systems, DLI must manage the vendor relationship to ensure continued value is provided. SITSD now provides various IT services after consolidation in 2022. During consolidation, DLI transferred 15 FTE to SITSD, which impacted staffing levels at TSD and could potentially create a reliance on SITSD and the UI vendor. While SITSD is not a vendor but rather a business partner, this relationship requires DLI to follow vendor management principles in order to manage the partnership and ensure its needs are being met. With various entities sharing responsibility for IT controls, managing these relationships is critical to maintaining security.

These new organizational changes also can impact the success of large IT initiatives, such as modernizing legacy systems and protecting citizen's data. To increase the success of these initiatives while maintaining an engaged workforce, DLI must commit to managing the organizational change, understanding where risks are, and navigating a service model no longer supported only by DLI.

Our audit focused on TSD's controls within processes and relationships critical to the success of DLI's modernization and security initiatives, including vendor, risk, security, IT service, and organizational change management. The scope of this audit includes the following:

- ◆ The shared structure of accountability, roles, and responsibility of key IT staff at DLI and SITSD within critical processes.
- ◆ Changes due to the 2022 IT service consolidation between DLI and SITSD.
- ◆ Review of contracts and agreements with UI vendor.
- ◆ Review of business partnership and agreements with SITSD.
- ◆ SITSD operations that directly support DLI IT operations related to critical processes, and
- ◆ MUSE implementation project.











What We Did

IT audit methodologies focus on reviewing process components to identify how capable they are of controlling risks. Risks to the agency are identified in planning and fieldwork. Fieldwork methodologies include:

- ◆ Identifying the individuals responsible and accountable for processes.
- ◆ Documenting a thorough understanding of control processes through interviews, observations, and document reviews.
- ◆ Reviewing any work products (reports, documents, decisions) or information sources related to reviewed processes.
- ◆ Identifying if there are metrics used for determining effectiveness.
- ◆ Surveying DLI employees to understand experiences related to IT services and changes.

As part of the audit, we determined how capable each control process is at meeting its intended goal and reducing risk to the agency. The following table (see page 4) summarizes the control areas reviewed during this audit and our overall determination. The control processes reviewed for each control area are discussed in greater detail in subsequent chapters:

Table 1
DLI Control Areas Summary

Control Process	Determination
Risk Management	0 
Security Management	0 
Leadership Accountability	1 
Vendor Management	1 
IT Service Management	1 
Organizational Change Management	1 
Legend	Process Capability
Activities are organized and the process is well-defined	3 
Basic activities are performed and are complete	2 
Some activity occurs, yet not organized or incomplete	1 
Incomplete or incapable process	0 

Source: Compiled by the Legislative Audit Division.

User Survey

During the audit, we surveyed 670 DLI employees. We received 500 responses for a response rate of 75%. We used the survey to understand DLI employees' experiences related to IT services and changes. Gap analysis compared DLI's activities to best practices, while survey information was used to understand the impact of findings on the user population. We asked respondents to rate their experience with the SITSD service desk, modernization happening in DLI, MUSE implementation, and TSD communication.

Criteria Used

State law outlines the responsibilities of all agencies to conduct IT resources in an organized, deliberative, and cost-effective manner. To successfully implement these requirements, IT governance and management practices are necessary. Therefore, both industry best practices and state requirements were used as criteria for this audit:

- ◆ The Montana Code Annotated (MCA) is a compilation of state laws. Specific IT and data statutes were referenced to identify agency roles and responsibilities.
- ◆ The Montana Operations Manual (MOM) contains policies, procedures, and standards applicable to state agencies. Risk management and staff evaluation policies were referenced.
- ◆ The Control Objectives for Information and Related Technology (COBIT) framework guides common IT management and governance practices to reduce technical issues and business risks. While DLI is not required to use this standard, the practices identified incorporate industry best practices. COBIT was used to evaluate organizational change (OCM), vendor, and IT leadership management practices. Other OCM best practice models, such as Prosci and the Kotter framework, were compared to COBIT and ultimately covered the same basic activities.
- ◆ The Information Technology Infrastructure Library (ITIL) is a set of detailed practices for IT activities such as IT service management that focus on aligning IT services with the needs of business. Again, DLI is not required to use this standard, but the practices identified incorporate industry best practices.

Chapter II – DLI’s Leadership Needs to be Accountable for Overall IT Control Structure

If prepared, DLI leaders are positioned to take on the challenges of sharing operational responsibilities with multiple entities. As the agency charged with carrying out a mission to serve the public, DLI is accountable for the success of IT initiatives and overseeing controls that reduce risk and ensure compliance. The leadership team at DLI, including division administrators and commissioner, play a crucial role in providing clear direction and ensuring staff are equipped to navigate change, meet stakeholder needs, achieve strategic goals, and maintain a control environment. When leadership demonstrates clarity and accountability, operational staff receive the necessary support and guidance to fulfill their duties and meet the agency’s objectives. To maintain this standard, it is essential that leaders also receive direction and feedback to set expectations and tone. Over the last three years, DLI has experienced turnover at the commissioner level and within executive leadership. DLI has struggled to follow the enterprise-wide evaluation process set in place by DOA and evaluate leadership based on all of their roles and responsibilities. Addressing these struggles will ensure DLI can better navigate changes, such as consolidation with SITSD, and ensure accountability for the overall IT control structure, no matter the turnover at any level.

The following table summarizes the review of leadership accountability and annual evaluation process at TSD.

Table 2
Leadership Control Processes

Control Process	Determination*
Leadership Accountability and Evaluation	
Annual Evaluation Process	Finding
Identified Roles & Responsibilities	Finding

Source: Compiled by the Legislative Audit Division.

* A pass/finding determination indicates whether process activities need improvement to meet the intention of the control area.

Significant Findings

In 2022, the Governor issued a directive for cabinet agencies to use the enterprise-wide performance evaluation system, conduct evaluations on an annual basis, and use general core competencies to evaluate employees. DLI did not follow this process during our audit period nor evaluate leaders on all aspects of their job responsibilities.

- ◆ In January 2024, DLI administrators received evaluations, but due to miscommunication in the commissioner’s office, they were not delivered until April 2024. Prior to this, DLI’s current TSD administrator had not received an evaluation since 2020.
- ◆ Leaders are evaluated on generic areas related to communication, integrity, and organization but fail to measure them against their specific roles and responsibilities. This is particularly important in IT due to the variety of stakeholders engaged with, high costs related to new systems, and data security needs.

COBIT's best practices indicate that IT leadership, in DLI's case, the TSD administrator, is accountable and responsible for many areas related to running an IT organization. They are responsible for managing vendor relationships and performance, as well as setting, measuring, and communicating IT strategy. To also be accountable, DLI's TSD administrator needs to ensure responsible parties are performing risk assessment and authorization duties, creating system security plans (SSP) and updates, and ensuring users receive timely and adequate IT support. The job standard that DLI relies on for the TSD administrator covers many of these areas but lacks key responsibilities in critical areas, especially those shared due to consolidation with SITSD. Agencies can include supplemental job information within the job standard to capture any additional work. However, areas of accountability and specific responsibilities related to vendor, risk, and organizational change management have not been defined for the TSD administrator. They are, therefore, not assessed through annual evaluations.

Impact

With leadership influencing all areas of an organization, the impact of undefined responsibility takes many forms. Ultimately, it has led to reliance on others to take responsibility, and shared control structures are unclear. This is seen in the other areas we evaluated and are discussed in detail later in the report.

Vendor and Service Management: The structure for vendor and business partner accountability is based on the direction provided by the Department of Administration's State Procurement Bureau through contract templates, not the internal strategy, business needs, and expectations of DLI. Therefore, key processes in which SITSD is providing a service, such as security, risk, and IT service management, are informal, unclear, and inconsistent. This increases the likelihood of risks that make the organization vulnerable and stakeholders frustrated.

Organizational Change Management: TSD relies on SITSD for strategic direction and expects other administrators to communicate their goals to DLI employees. TSD's incomplete change management program has led to unclear leadership responsibilities related to managing change, such as establishing implementation teams, preparing stakeholders for change, holding new process owners accountable; inconsistent communication with stakeholders; and performance measurement of the IT strategy.

Improvement Opportunity

The Governor directive and MOM performance evaluation policy require agencies to evaluate employees annually. When followed, this can help ensure consistency even when organizations face turnover. In 2021, the governor appointed a new DLI commissioner who served until June 2023. After their departure, the chief of staff acted as commissioner until August 2023, when the current commissioner was brought on. In January 2024, the chief of staff, who was hired in February 2021, conducted evaluations of DLI administrators due to their familiarity with the leadership team and having a new commissioner. However, the chief of staff then left DLI in January 2024.

Additionally, the previous TSD administrator left the position in January 2022. The current administrator was temporarily promoted at that time and permanently promoted in December of 2023. This turnover, coupled with miscommunications, resulted in evaluations not being distributed until April 2024.

DOA provides general core competencies for agencies to use to evaluate employees. In addition to these, agencies can provide more detailed job expectations through goal setting in the evaluation process. By using the job standard, with the supplemental job information, to guide performance evaluations, DLI can ensure that all aspects of a job are reviewed and employees have a complete evaluation.

DLI did not follow the enterprise-wide evaluation process and could not consistently hold leadership accountable or provide valuable and specific feedback. Following the established process and building off of the general core competencies, DLI can help ensure accountability is held even through commissioner turnover and large-scale IT changes.

RECOMMENDATION #1

We recommend the Department of Labor and Industry follow the statewide performance evaluation process and ensure:

- A. *Roles and responsibilities related to risk, vendor, and organizational change management programs are addressed in the Technology Services Division Administrator's occupational standard and,*
 - B. *Regularly evaluate agency leadership based on occupational job standards.*
-

Chapter III – DLI and SITSD Need to Define Responsibilities in the Shared IT Control Structure

DLI, SITSD, and the state are embracing a vendor-first approach for IT systems and services, marking a significant shift in strategy. While this approach offers benefits, it underscores the need for robust management practices to align with the IT strategy and ensure performance and shared responsibilities are defined. DLI is uniquely positioned under SITSD’s oversight while being a customer of its operational services following the 2022 IT service consolidation. SITSD is a business partner rather than a vendor to DLI, but there are similarities in how they are managed as they ensure needs are being met. Other agencies rely on SITSD for infrastructure, network management, and essential tools. However, these agencies have not yet consolidated procedural-based risk and security management operations. This shift in responsibilities from the agencies to SITSD significantly changes the shared IT control structure and impacts the relationship between them. Successfully managing this and clearly defining shared responsibilities is essential for the effectiveness of DLI’s risk, security, and IT service management programs.

Table 3
Shared Responsibility Control Processes

Control Process	Determination*
Vendor Management	
Vendor Selection	Pass
Contract Management	Finding
Performance Monitoring	Finding
Relationship Management	Finding
Vendor Risk Management	Finding
Continual Improvement	Finding
Risk Management	
Risk Management Framework	Finding
Roles and Responsibilities	Finding
Security Management	
Security Roles and Responsibilities	Finding
New Application System Security Plan	Finding
IT Service Management	
Plan	Pass
Improve	Finding
Engage	Finding
Design and Transition	Finding
Obtain/Build	Finding
Deliver and Support	Pass

Source: Compiled by the Legislative Audit Division.

* A pass/finding determination indicates whether process activities need improvement to meet the intention of the control area.

Inconsistencies in how DLI manages vendors and their partnership with SITSD have led to contrasting engagements. DLI has completed structured projects, like MUSE but lacks structure with other service relationships, including SITSD. This inconsistency in managing engagements and establishing a shared responsibility model has impacted further areas of IT, as shown in our assessment summary (Table 3).

Significant Findings

COBIT and ITIL best practices stress the importance of having a holistic vendor management program. These areas (identified in Table 3) ensure organizations consistently manage external relationships with clear communication, roles, responsibilities, and deliverables. Rather than having this formal structure, DLI relies on contract statements of work (SOWs), the Department of Administration’s State Procurement Bureau (SPB), and SITSD to guide their relationships. This leaves the service or product largely the provider’s responsibility without consistent oversight of the relationship and services.

Due to this reliance on the SOW and the vendor's experience in providing these services and products, DLI could hold the new UI system, MUSE, and vendor accountable for project deliverables related to its implementation. DLI managed the contract, monitored performance during the project, consistently communicated, and identified and remedied risks associated with the implementation. However, not all DLI engagements have an SOW in place with a well-defined relationship.

DLI and SITSD do not have an SOW, contract, or a similar alternative to guide and manage the business partnership and clarify areas of authority, responsibility, performance, and risk. Since the consolidation in 2022, DLI has relied on SITSD to manage risk, security, and IT service programs. SITSD provides IT services such as helpdesk support to DLI, yet lacks direction on how to coordinate with and support DLI in implementing a risk management framework and developing SSPs.

Impact

Because DLI shares various responsibilities with SITSD, there are significant impacts across the business that users ultimately feel. The roles and responsibilities of DLI's risk and security management programs are undefined, and services meant to secure data have been delayed. IT service responsibilities between DLI and SITSD are unclear, and users are caught in the middle—thus impacting the agency in critical areas.

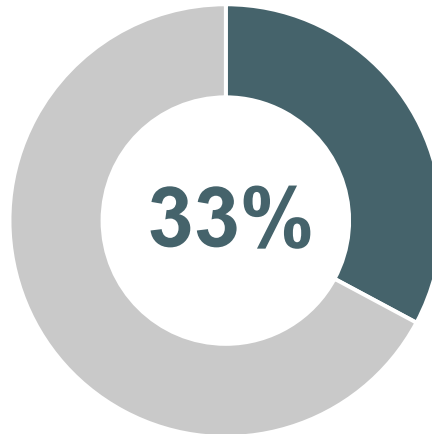
Security Management: As part of federal guidance, a social security crossmatch should be in place for state UI systems. All requisite security responses and documentation must be reviewed and approved to set this up. Delays in providing this information prevented this crossmatch from being in place at launch. SITSD did not have a final SSP for MUSE until three months after launch, and the crossmatch went live in March 2024, five months after launch.

Risk Management: New systems, such as MUSE, need an authorization to operate (ATO) signed by the State CIO. ATOs document that risk at the system level is being managed. Due to unclear responsibilities between DLI and SITSD, the ATO was not signed until January 2024, meaning MUSE was operating for three months without official authorization. At the end of the audit, DLI indicated it is currently working with DOA to hire a position back at DLI that would coordinate security and risk management on the agency side.

IT Services Management: DLI employees have faced disruptions in their IT services, which has impacted the overall user experience with IT, including the perception of major IT projects and consolidation with SITSD. MUSE met its implementation deadline. Yet, responses gathered from our survey show that 40% of users rated the launch as either slightly successful or not at all. Half of the comments we received about the launch discussed how the perception of the system was not ready at launch, with various aspects of the system not working, needing to be fixed, or the overall project being rushed to meet a deadline. 86% of respondents rated IT support provided by SITSD as "Moderately effective" or better. However, feedback channels during the transition were lacking as shown in Figure 3 (page 11).

Figure 3
Inadequate Feedback Channels

A third of respondents felt there were inadequate channels for feedback during the transition of IT services.



Source: Compiled by the Legislative Audit Division.

Improvement Opportunity

In general, DLI needs to incorporate vendor management practices specific to evaluating overall vendor performance and compliance with contract requirements, facilitating communication with internal and external stakeholders, coordinating feedback on services, and implementing a continual improvement process for managing service-provider relationships. These practices along with those directed by SPB and SITSD will further improve how the agency manages external relationships, including their partnership with SITSD. DLI's unique situation of having SITSD take on a more active role in operations has confused responsibility between the two. Management practices focused on clear roles, and ownership should be in place for the partnership with SITSD to maintain a positive DLI staff experience with IT while meeting business needs.

RECOMMENDATION #2

We recommend that the Department of Labor and Industry take accountability in the shared control structure and improve relationships by:

- A. *Incorporating aspects of vendor management best practices such as deliverable management, performance monitoring, and relationship management into DLI policy and procedures and,*
- B. *Work with the Department of Administration to develop a formalized shared responsibility model.*

SITSD Opportunity for Improvement

Our criteria for this work relied heavily on best practices rather than MOM policy. This is because SITSD has not provided agencies with guidance related to vendor management. As IT solutions become more complex, provide more services, and involve areas of new technology, vendor management becomes essential in maintaining a shared control environment with an external entity.

Additionally, when SITSD is a business partner that provides services, the relationship with agencies changes. As more consolidation projects occur with other agencies, SITSD can help them understand and navigate this new partnership by coordinating and establishing roles and responsibilities. Agencies need to be accountable and ensure SITSD is responsible for deliverables while clearly understanding what is still the agency's responsibility. Using leadership job standards, an agency can be accountable for its role. A memorandum of understanding, or something similar, between SITSD and agencies can make clear what is and is not SITSD's responsibility. As a governance body, SITSD can help agencies manage these changes and the increase in vendor usage.

RECOMMENDATION #3

We recommend that the Department of Administration, in conjunction with the State Procurement Bureau, help agencies prepare for increased vendor and State Information Technology Services Division (SITSD) engagement by:

- A. *Providing agencies shared responsibility guidance and,*
 - B. *Establishing a formal agreement with clear roles and responsibilities when SITSD is providing services and sharing responsibility for security controls.*
-

Chapter IV – Improved Organizational Change Management Is Needed for DLI to Transform IT

Organizational change management (OCM) is the driving force behind the success of all major organizational decisions and strategic directions. It helps ensure personnel, from leadership to staff, are held responsible, progress on goals is measured, and stakeholders are involved and updated on progress. As noted previously, by not managing IT service consolidation changes with SITSD, DLI has faced numerous issues with their risk, security, and IT service programs that have experienced major changes. SITSD and TSD IT goals should align, but that does not remove the necessity for TSD to manage its goal creation and change processes. TSD leadership has an opportunity to develop and ensure its strategic direction is prioritized while still aligning with statewide goals. It has aspects of a structured process, but improvements are needed to ensure accountability, performance measurement, and communication with stakeholders.

The following table summarizes the review of TSD’s OCM process.

Table 4
Organizational Change Management Control Processes

Control Process	Determination*
Managed Organizational Change	
Establish the Desire to Change	Finding
Form an Effective Implementation Team	Finding
Communicate Desired Vision	Finding
Empower Role Players and Identity Short-Term Wins	Finding
Enable Operation and Use	Finding
Embed New Approaches	Finding
Sustain Changes	Finding

Source: Compiled by the Legislative Audit Division.

* A pass/finding determination indicates whether process activities need improvement to meet the intention of the control area.

Significant Findings

TSD has various aspects of a successful OCM process but does not include all areas to ensure a consistent approach. It relies on SITSD to guide the goal-setting process but struggles to balance its needs and statewide needs. TSD works with other divisions and the Commissioner to develop DLI IT goals and objectives. However, these do not align with best practices. Goals should be specific, measurable, achievable, relevant, and time-bound (SMART). DLI IT goals lack this specificity and make it difficult to measure incremental progress.

TSD has demonstrated communicating its goals with DLI leadership. Despite this, it has shown inconsistencies with goal communication. During the audit, TSD’s goals on its website did not align with what was provided to the audit team. The goals were last updated in 2021. TSD has aspects of proper OCM but lacks a formalized documented process to ensure this is repeatable and improvements can be made.

Best practices outline the necessary steps to ensure a holistic and consistent approach to major changes is achieved. The following sections represent those steps and are accompanied by TSD's adherence to them through the implementation of MUSE and consolidation of services with SITSD.

Desire to Change: Stakeholders must be prepared for and accept change. TSD, in conjunction with SITSD, identified the need for IT service consolidation with SITSD. However, the impact was not fully evaluated, and communication was inconsistent.

Implementation Team: Effective implementation teams help establish common goals and build trust across organizations during times of change. TSD established the goal of consolidation, but a team was not established.

Communicate Vision: The rationale, benefits, and impact of changes must be communicated to stakeholders. TSD is inconsistent in its goal communication and expects other DLI divisions to communicate TSD goals.

Empower Role Players: Training stakeholders is essential for ensuring changes are successful. TSD highlighted the importance of training IT staff via their strategic goals. Training plans for MUSE users were identified and implemented. However, training related to new IT service consolidation processes was not established, demonstrating TSD's lack of consistency in this area.

Enable Use: Plans must be established to address all technical, operational, and usage aspects of the change. While there are plans to use MUSE, there is no plan for handling consolidation.

Embed New Approaches: New process owners need to be held accountable. Roles and responsibilities between DLI and SITSD have not been established for security and risk management. Key documents, such as the ATO and SSP for MUSE, were not finished until several months after the system was implemented.

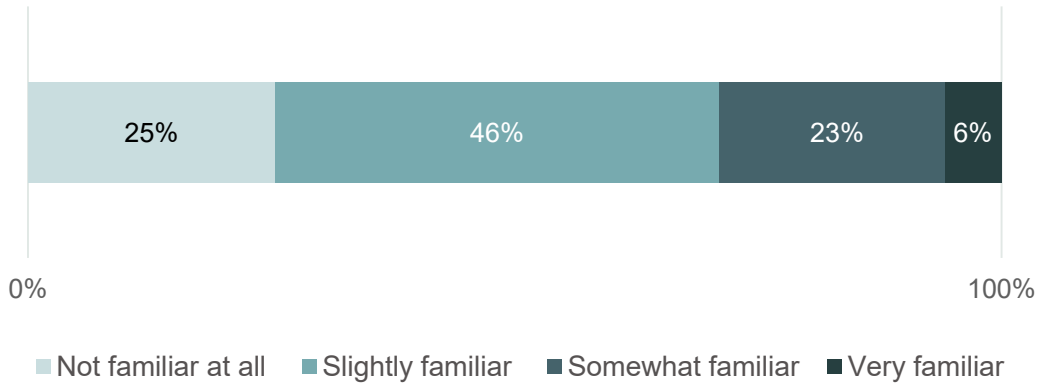
Sustain Changes: Ongoing communication, commitment from top management, and measurement of success should occur. TSD updates its goals once a year but with only a bulleted list and lacks metrics. These are then distributed to DLI administrators. There are review mechanisms for in-house DLI applications and MUSE but not for other strategic goals such as consolidation.

Impact

OCM is the process of managing the changes that SITSD and TSD have gone through related to risk, security, and IT service management, as seen in the previous chapter, this has impacted DLI operations. The figure below shows survey information related to stakeholder familiarity with IT modernization in their divisions.

Figure 4
User Familiarity with IT Modernization

Over 70% of respondents were, at best, only slightly familiar with IT modernization in their division.



Source: Compiled by the Legislative Audit Division.

In addition to this, Figure 3, on page 11 of the report, highlights that a third of respondents felt there were inadequate channels for feedback during the transition of IT services. Part of this confusion is attributed to a lack of a communication plan and strategic performance measures. IT strategic goals are not consistently measured, which hampers TSD’s ability to determine initiative success and keep stakeholders updated on progress.

Improvement Opportunity

While TSD has shown us their goal setting process, improvements are still needed in communication, performance measurement, and formalizing roles and responsibilities. DLI leadership should take a more prominent sponsorship role and establish a structure for significant changes. By having documented procedures related to getting stakeholder buy-in, establishing and empowering implementation teams, embedding new approaches, and communicating a shared vision, DLI can ensure a strong foundation is in place to manage major efforts for IT modernization.



RECOMMENDATION #4

We recommend that DLI strengthen its organizational change management by implementing a best practice framework and ensuring the following is documented and formalized

- A. *Roles and responsibilities within TSD and DLI management,*
- B. *IT strategy and goal communication plan with stakeholders, and*
- C. *Performance measurement of the IT strategy.*



DEPARTMENT OF
LABOR AND INDUSTRY

DEPARTMENT OF
ADMINISTRATION

DEPARTMENT RESPONSES



August 16, 2024

Angus Maciver, Legislative Auditor
Legislative Audit Division
Room, 160, State Capital
PO Box 201075
Helena, MT 59620-1705

RECEIVED
August 16, 2024
LEGISLATIVE AUDIT DIV.

RE: Department of Labor & Industry and Department of Administration Response to Legislative Audit Division *Vendor-First Approach to Agency IT Services: DLI Test Case for Controlling Shared Services* Audit Findings

Dear Mr. Maciver:

The Department of Labor & Industry (DLI) has reviewed the Vendor First Approach to Agency IT Services audit. DLI thanks your staff for their review. DLI welcomes collaborative opportunities to improve DLI operations. Our responses to LAD's recommendations are as follows:

Recommendation #1

We recommend that the Department of Labor & Industry follow the statewide performance evaluation process and ensure:

- A. Roles and responsibilities related to risk, vendor, and organizational change management programs are addressed in the Technology Services Division Administrator's occupational standard and,
- B. Regularly evaluate agency leadership based off of occupational job standards.

Response:

Do Not Concur

DLI currently follows statewide performance evaluations processes. DLI utilizes and evaluates employee performance, based on approved Department of Administration (DOA) occupational standards for all DLI positions including those in IT, as required by State policy published in the Montana Operations Manual (MOM). Current DOA approved occupational standards for an IT Executive require direct management over all aspects of IT activities, including those specified in Recommendation #1 – risk, vendor, and organizational change management – as well as integrations, development and sustainability of security risk strategies, and management of external agency partners. These standards act as the foundational metrics for evaluating agency IT Executive job performance.



DLI has faced significant transition in the Commissioner's Office, with six Commissioners in seven years electing not to conduct performance evaluations of senior agency staff. At my request upon my appointment, previous Acting Commissioner Elizandro completed 2023 performance evaluations, and I will complete 2024 evaluations using approved DOA forms.

Recommendation #2

We recommend the Department of Labor & Industry take accountability in the shared control structure and improve relationships by:

- A. Incorporating aspects of vendor management best practices such as deliverable management, performance monitoring, and relationship management into DLI policy and procedures and,
- B. Work with the Department of Administration to develop a formalized shared responsibility model.

Response:

Do Not Concur

Prior to initiation of the audit, Deloitte assessed DLI's IT practices to develop a strategy for planned updates and improvements. As conveyed to LAD throughout the audit, based on Deloitte's assessment and recommendations, DLI utilizes an Enterprise Project Management (EPM) framework as the foundation for managing IT projects. EPM's framework aligns with industry standard best practices, while focusing on the value and impact of IT projects on DLI functions and State systems as a whole. This translates into multiple projects running concurrently as compared to a traditional vendor management process which focuses on one project result. The EPM framework drives a top-down governance that encompasses all program and project implementation while promoting a cultural shift from siloed to integrated activities. EPM is the basis for the creation of all DLI IT project Statement of Works (SOW), including SITSD consolidation. The EPM approach directed by Deloitte, drives the delineation of roles and responsibilities for all stakeholders throughout IT project life cycles.

The consolidation of DLI IT programs into SITSD is an extension of services SITSD currently provides through the fixed cost model. IT specific fixed costs includes various operational services and support to all state agencies, which does not require formal agreements. The inclusion of DLI help desk support, system administration, and security operations further mitigates risks associated with siloed IT activities between agencies. Successful migration of these processes into SITSD operations has been a shared responsibility with on-going efforts. LAD staff was informed during the audit that DLI and SITSD were conducting Risk Management Consolidation Discovery workshops focusing on processes which have experienced migration challenges. Exhibit A documents the results of the first security risk assessment meeting, formalizes additional plans for security risk assessment, outlines shared roles and responsibilities for implementation and sets future meeting dates.



Overall, DLI has successfully met IT industry standards by incorporating the EPM framework for multiple IT projects which includes the Employment Standards Division's Acella system, the new Workforce Service Division case management EmployMT system, and the new Unemployment Insurance Division MUSE system.

Recommendation #3

We recommend that the Department of Administration, in conjunction with the State Procurement Bureau, help agencies prepare for increased vendor and State Information Technology Services Division (SITSD) engagement by:

- A. Providing agencies shared responsibility guidance and,
- B. Establishing a formal agreement with clear roles and responsibilities when SITSD is providing services and sharing responsibility for security controls.

Response:

Concur

Please see DOA's response to this recommendation.

DLI concurs with DOA, that both SPSD and SITSD should continue to enhance vendor management guidance and expectations for all agencies, including DLI. Providing robust guidance will help align roles and responsibilities between SITSD and state agencies, including DLI, further mitigating risks for all stakeholders and customers.

Recommendation #4

We recommend that DLI strengthen its organizational change management by implementing a best practice framework and ensuring the following is documented and formalized:

- A. Roles and responsibilities within TSD and DLI Management
- B. IT Strategy and goal communication plan with stakeholders, and
- C. Performance measurement of the IT strategy

Response:

Partially Concur

DLI engaged Deloitte, a contracted objective vendor, to assess DLI's IT functions and develop an IT Strategy. Deloitte's assessment of DLI TSD processes resulted in a recommendation to develop and implement an EPM framework. As noted in DLI's response to Recommendation #2, DLI has successfully partnered with DOA to implement an EPM framework for simultaneous initiation and management of multiple IT projects. However, DOA is not a vendor and is not subject to DLI's vendor management strategies. DOA and DLI are partners in IT functions. The EPM framework provides a holistic approach to planning for and implementing IT projects. The partnership approach between DLI and DOA mitigates risks of program overlap. Components of these projects include GAP identification, extending the scope of mitigation to include staff resiliency, reduction of technical debt, leveraging of cloud hosted resources, communication enhancements, continued



modernization of existing systems, and identification of IT strategy specific performance metrics. DLI continually plans, sets, and progresses towards IT needs to strategically maintain stable, secure, and modern technical systems, while leveraging the Enterprise platforms and State IT Strategies.

As a component of the EPM framework, DLI will continue to align established DLI goals and objectives into various enterprise-wide IT project plans. Additionally, DLI remains committed to enhancing operational communications among all stakeholders to ensure appropriate engagement and alignment.

As additional support and consideration of joint commitments to ongoing partnership, DLI and STISD are providing in Exhibit A, identified challenges, observations, and considerations not addressed or presented in LAD's report.

Respectfully,

A handwritten signature in black ink, appearing to read "Sarah Swanson". The signature is fluid and cursive.

Sarah Swanson, Commissioner
Montana Department of Labor & Industry



Exhibit A

Risk Management Security Consolidation Discovery Workshop

Workshop Overview and Outputs:

The intent of these workshops is to identify gaps from the previous consolidation attempt in order to address a path forward. The first four workshops will focus specifically on **Risk Management Security Consolidation** and will closely model the work SITSD is doing with other agencies across the enterprise. As a result of these initial Risk Management workshops, DLI can expect the following outputs:

- A detailed Gap Analysis.
- A Service Level Agreement with a RACI matrix for the identified shared responsibilities.
- A MOU (this may look different for DLI and will most likely include agreements for the other services being consolidated).
- An implementation roadmap.

In conjunction with this work, SITSD is currently assessing and mapping out a plan for the rework that will need to occur in other tech service areas, including Service Desk, Server Hosting, and Desktop Support. Additional workshops will be scheduled in later weeks to discuss these services separately where the correct subject matter experts can be present to assist with planning. The ultimate goal is to have a roadmap for the rework for all services by December 31, 2024.

Workshop Schedule

July 22nd – Risk Management (Consolidation & Future) – Below framework results from this initial workshop.

August 21st – Overview of DLI's business and mission, Agency risk assessment, understanding current security status through a security snapshot, understanding current vulnerability

August 9th – TBD – Service Desk, Serner Hosting, and Desk Top Support

October 2nd – TBD – Service Desk, Serner Hosting, and Desk Top Support

What does Consolidation mean in the context of Risk Management Security?

- Consultation- dedicated ISSO's from SITSD to guide DLI through processes and requirements.
- Initiation- scheduling discovery workshops, identifying resources, meeting with agency Director.
- Discovery- workshops focusing on cyber hygiene, system and agency risk assessments, vulnerability management, and a general overview/understanding of the Risk Management Framework.
- Implementation- a roadmap delivered within 60 days of completion of the discovery workshops identifying milestones to get DLI to the desired future state.



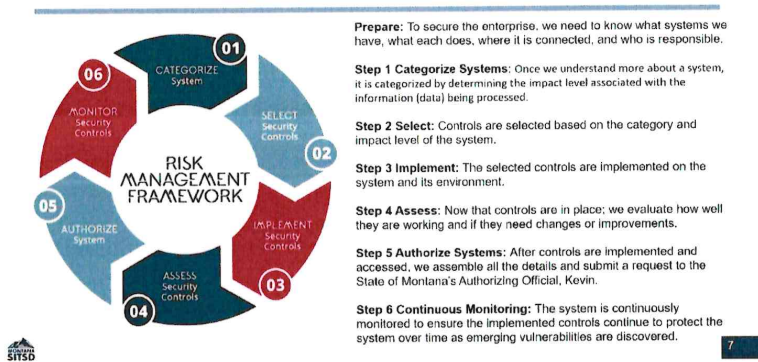
- Stabilization- Continuous monitoring of systems and packages including periodic review of areas where gaps were initially identified.

Risk Management Framework (RMF) Review:

During these workshops, we will focus on the “Prepare” step of the RMF, outlined below. Integrity and availability of the data on DLI’s systems is critical. During the prepare step, we will focus on the following:

- Identifying system inventories.
- Identifying stakeholder roles (System Owners, Business Owners, etc.).
- Continuous Authorization to Operate (ATO) instead of point in time security.
 - o Security by design as part of the State IT Strategy.
 - o Feedback loops are always updated.
 - o Continuous monitoring for all systems and packages rather than every three years.
 - o Grouping of similar systems under one ATO with one set of controls (federally regulated data will have its own ATO).

RISK MANAGEMENT FRAMEWORK



Goals for SITSD:

- Gain a better understanding of DLI’s business and purpose.
- Complete risk assessments for both agency as a whole and identified critical systems.
- Identifying critical systems in need of System Security Plans (SSPs) and ATO’s.
- Build relationships to become a trusted security advisor.

Goals for DLI:

- Clear understanding of where roles and responsibilities will lie in the future state.
 - o Roles should be documented (Includes TSD Administrator)



- A shared understanding of terms (ATO, SSP, Risk Assessment, System Owner, etc.).
- Data kept in spreadsheets will be moved into systems DLI is currently utilizing.
- Improved inventory management.
 - o ServiceNow Discovery, Tanium, APM. How do all these fit together and how does data flow between systems?

Milestones and KPI's:

- Ongoing risk assessment results.
- Improved Archer utilization.
- Improvement effectiveness in Vulnerability Management.
- Improvement in inventory accuracy.
- Improve user education.
- Implementing secure procurement practices.
- Customer satisfaction.

Roles & Responsibilities - SITSD Support Services for DLI

1. Desktop Support Services Section:

Provides support functions for desktop services, including imaging, inventory, patching, deploying applications, troubleshooting desktop issues and decommissioning of end-of-life desktops. Provide support and guidance for users of VPN and VMWare virtual desktop environments. Strategize and deploy future desktop service software and applications based on business needs.

2. IT Service Desk Section:

Provides first-line IT service desk support, including multi-factor identification issues and assignment of multi-factor tokens (or other hardware), email management, password resets, and other general IT inquiries. May refer incidents to second-level support (Desktop Support or other) for highly technical or high security access issues.

3. Enterprise Customer Workflows Bureau:

Provides business analyst services to end users to develop work-flow processes to enhance business objectives and improve business performance. Build digital workflows based on set standards created through the business analysis process using the ServiceNow platform.

4. Application Development Operations Section:

Develop, maintain, edit and support web portals such as websites, intranet and more. Create, maintain and assist customers with web content, website templates, web browsers, web analytics graphic tools and other related internet technologies. The majority of this work will be created using the statewide web content management system, Cascade CMS.



5. Application Hosting Section:

Support a variety of application technologies in test, development and production environments including web servers, Java and .Net application servers and numerous commercial software packages. Support includes implementation design, technical support, software installation and maintenance and performance monitoring and tuning.

6. Enterprise Infrastructure Services:

Implement, manage, configure and monitor automated private cloud infrastructure. Create and maintain scripts and workflows necessary to support cloud environments. Diagnose problems and find resolutions to systems issues, monitor systems and identify opportunities to grow cloud services.

7. IT Security:

Provide full-service IT security to protect data. Utilize cybersecurity standards, guidelines, best practices and the NIST Cybersecurity Framework. Perform proactive and reactive cyber security duties such as incident response, threat hunting, automation, threat intelligence analysis and continuous monitoring. Oversee, evaluate and support creation of documentation, validation, assessment and authorization processes for network and information systems security.

Overall – Key factors report did not highlight

1. Successful Implementation Despite Challenges

The projects named (specifically MUSE) provided all the necessary functionality to enable business continuity while replacing failing systems. Despite the challenges and issues highlighted, the projects ultimately met their primary objectives.

- **Functional Success:** The primary goal of any IT project is to ensure that the new system meets the functional requirements and supports business operations effectively. The successful implementation of the Montana Unemployment Services Environment (MUSE) and other systems demonstrates that DLI achieved this goal, ensuring continuity and improving service delivery.
- **Modernization Success:** DLI will be the first agency to eliminate the majority of technical debt brought about by old and aging systems. In some instances, this came just in time. For example, the month before the old UI system was retired, unemployment checks were delayed due to problems with the system that were getting worse. MUSE enabled resumption of mission critical work. This has been followed by the transition of other systems that are too old and present maintainability problems that include security concerns.



2. Importance of Timely Completion

The audit report criticizes the push to complete projects on time, suggesting that it may have led to issues such as inadequate feedback channels and incomplete security documentation. However, in addition to replacing systems that break and endanger the Agency's ability to deliver mission-critical services, there are other reasons for pushing toward a deadline with an MVP approach:

- **Timely Delivery is Critical:** Completing projects on time is crucial for several reasons, including minimizing disruptions, avoiding additional costs, and maintaining stakeholder trust. Delays can lead to extended periods of operational inefficiency and increased costs, which can be more detrimental than the issues arising from a tight schedule.
- **Managing Risks and Costs:** Timely project completion helps in managing costs effectively. Delays often result in cost overruns due to extended use of resources, additional labor costs, and potential penalties. By adhering to the project timeline, DLI managed to avoid these financial pitfalls.

3. Effective Project Management Practices

DLI has worked with internal partners such as SITSD and vendors to ensure effective project management practices contribute to the successful implementation of the projects:

- **Clear Objectives and Planning:** The projects had clear objectives and were planned to ensure that all critical functionalities were delivered. This aligns with best practices in project management, which emphasize the importance of clear planning and objective setting.
- **Resource Allocation and Monitoring:** DLI effectively allocated resources and monitored project progress to ensure that deadlines were met. This proactive approach is essential in managing large-scale IT projects and mitigating risks associated with delays.

4. Continuous Improvement and Learning

The report also fails to point out that the approach taken to quickly stand-up systems and continuously improve are, in fact, best practice. Some considerations of this approach include:

- **Feedback and Adjustments:** While the audit report points out issues with feedback channels, DLI has taken steps to improve these processes based on the lessons learned from previous projects. Continuous improvement is a hallmark of effective project management and demonstrates the DLI's commitment to refining its practices.



- **Adapting to Changes:** DLI has shown adaptability in managing changes and addressing issues as they arise. This flexibility is crucial in the dynamic environment of IT projects, where unforeseen challenges are common.

In addition to the issues listed above, there are potentially methodological problems with the audit process. The survey methodology used in the audit report did not adequately consider several critical factors that could have influenced the survey responses. These factors include the impact of new systems on highlighting existing issues, disgruntled employees due to previous system failures, and outdated processes that posed significant risks. Here are the key points:

1. Disgruntled Employees Due to Previous System Issues

One item to consider when evaluating survey response is that some employees might have been disgruntled due to:

- **Accountability Issues:** Employees might have been accustomed to a lack of accountability due to the old systems not tracking work correctly. The new systems, which introduced better tracking and accountability, could have been perceived negatively by those who were not used to being held accountable for their work.

2. Outdated Processes and Risks

The audit report did not fully account for the risks associated with outdated processes that the new systems aimed to address. These outdated processes included:

- **Lack of IT Change Management:** The absence of a formal IT change management process meant that every change posed a risk to the systems. This lack of structure could have led to frequent issues and disruptions, which the new systems aimed to mitigate.
- **Inadequate Ticketing System:** The previous lack of a proper ticketing system for IT issues meant that problems were not tracked or resolved efficiently. The new systems introduced better processes for managing IT issues, which could have been seen as disruptive by employees used to the old ways.

3. Impact on Survey Responses and Findings

These factors are important because they directly impact the validity of the survey responses and the overall findings of the report:



- **Bias in Responses:** Employees who were disgruntled due to previous system issues or who were resistant to the new accountability measures might have provided biased responses. This bias could have led to an overly negative portrayal of the new systems' effectiveness.
- **Highlighting Existing Issues:** The new systems likely highlighted existing issues that were previously hidden or ignored. This exposure could have led to initial resistance and negative feedback, as employees adjusted to the new processes and accountability measures.
- **Underestimating Improvements:** The survey methodology might not have fully captured the long-term benefits and improvements brought by the new systems. Initial resistance and adjustment periods are common with any significant change, and the survey might have been conducted too soon to reflect the true impact of the new systems.



MONTANA DEPARTMENT OF ADMINISTRATION

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

doa.mt.gov
406.444.2460
doadirector@mt.gov

August 16, 2024

Angus Maciver
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620

RECEIVED
August 16, 2024
LEGISLATIVE AUDIT DIV.

Re: *23DP-03-DOA Vendor-First Approach to Agency IT Services: DLI Test Case for Controlling Shared Services*

Dear Director Maciver,

The Department of Administration (DOA), State Procurement Services Division (SPSD), and State Information Technology Services (SITSD) have reviewed the Audit report. We appreciate the insights provided by the audit and are committed to implementing the necessary changes to enhance our processes.

You had one recommendation directed to DOA including both SPSP and SITSD. Our response is as follows:

Recommendation #3: Governance, risk assessment, and planning

The Department of Administration, in conjunction with the State Procurement Bureau, needs to provide guidance and expectations to agencies on how manage vendors. When providing services and sharing security responsibilities with agencies, the State Information Technology Services Division needs to establish clear roles and responsibilities.

Department Response: The Department concurs with this recommendation. The Department expects to complete the work detailed below by December 31, 2025.

1. Vendor Management

As part of our procurement modernization efforts, DOA SPSP continues to improve its guidance and expectations to agencies on vendor management. In the next year, DOA SPSP plans to review our current vendor management guidance and determine how to update and enhance this guidance. The main objectives of vendor management from a procurement perspective include:

- *Vendor and Contract Management*: This includes ensuring the selection, initial contract, amendments, and renewals meet the agency's needs, and complies with statute, rules, and policy.
- *Risk Management*: Identifying, assessing, and mitigating risks associated with vendors to protect the organization's operations and reputation. This involves monitoring compliance, data security, and potential supply chain disruptions.
- *Performance and Contract Monitoring*: Tracking vendor performance to ensure they meet contractual obligations and quality standards. This includes regular performance reviews, feedback sessions to identify areas for improvement, and documentation of the feedback.
- *Relationship Management*: Building and maintaining strong, collaborative relationships with vendors to foster trust and loyalty. This involves open communication, joint problem-solving, and strategic partnerships that can lead to innovation and mutual benefits.

2. Service Delivery and Shared IT Security Functions

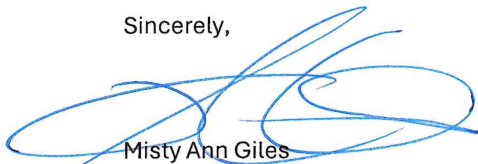
As part of our service delivery and risk management security consolidation, SITSD plans to ensure that roles and responsibilities are clearly defined.

- *Risk Management Security Consolidation*: As part of the ongoing risk management security consolidation, SITSD and each consolidated agency agrees to defined roles and responsibilities for risk management functions.
- *Service Level Agreements (SLAs)*: Initiate a comprehensive review of all existing Service Level Agreements (SLAs) to identify any discrepancies or areas lacking clarity in current SLAs, ensure they clearly define roles and responsibilities, and engage with agencies to ensure all concerns are addressed in the SLAs.

By implementing these actions, we aim to enhance our procurement processes and align them with best practices, thereby increasing efficiency and reducing risks. We are confident that these changes will address the concerns raised in the audit and improve our overall operations.

Thank you for your guidance and support. We look forward to working collaboratively to ensure the highest standards of procurement and IT services.

Sincerely,



Misty Ann Giles
Director, Department of Administration