A Report
to the
Montana
Legislature

Information Systems Audit

The Montana Enhanced Registration and Licensing Information Network (MERLIN)

Department of Justice

September 2022

Legislative Audit
Division

21DP-01

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
Jemma Hazen
William Hallinan
Tyler Julian

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

September 2022

The Legislative Audit Committee
of the Montana State Legislature:

This is our Information Systems compliance audit of the Montana Enhanced Registration and Licensing Information Network (MERLIN) system managed by the Motor Vehicle Division and Justice Information Technology Services Division within the Department of Justice.

This report provides the Legislature information about the governance and management practices intended to ensure MERLIN is meeting the needs of users and other requirements. This report includes recommendations for improving general controls with more comprehensive, managed processes within IT human resources, risk, and security as well as developing an IT governance structure within the Department of Justice. A written response from the Department of Justice is included at the end of the report.

We wish to express our appreciation to Department of Justice 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

Tables

Elected, Appointed, and Administrative Officials

Department of Justice Austin Knudsen, Attorney General

Will Selph, Chief of Staff

Stephanie Cote, Administrator, Central Services Division

Michael Harris, Administrator, Justice Information Technology Services Division

Lauri Bakri, Administrator, Motor Vehicle Division

MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS COMPLIANCE AUDIT

The Montana Enhanced Registration and Licensing Information Network (MERLIN)

DEPARTMENT OF JUSTICE

A report to the Montana Legislature

BACKGROUND

The Montana Enhanced Registration and Licensing Information Network (MERLIN) system is administered by the Motor Vehicle Division (MVD) of the Montana Department of Justice (DOJ). MERLIN is a large and complex system that incorporates multiple functions such as vehicle title and registration, financial and accounting processes, and dealer licensing and inventory to manage MVD's business processes.

Montana has more than 1.75 million titled vehicles and MERLIN supports the yearly task of providing titles for 470,000 vehicles, registration for over 1 million vehicles, and licenses and ID cards for approximately 200,000 individuals per year. MVD generates approximately $180 million annually with a $11 million operating cost.

MVD revenue:
FY21 $176,396,660
FY22 $172,496,519

Justice Information Technology Services Division (JITSD) is rebuilding information technology (IT) management to define policies and procedures, determine roles and responsibilities, and run day-to-day operations. However, it has struggled with organizing and defining management practices. DOJ does not have a structure of IT governance to provide direction, which limits JITSD's ability to support agency goals, provide services, and meet requirements. Without improvements, the MERLIN replacement project is at risk of not meeting goals and the new system is more likely to see issues with meeting federal requirements and users' needs.

COMPLIANCE SUMMARY:

Focus Area	Rating
IT Governance	**Unsatisfactory**
The combination of process maturity and effect of findings is not acceptable considering the context of the agency, data, or services provided.	
IT Management Framework	**Needs Improvement**
Processes may exist; however, the lack of maturity has negative effects and needs to be addressed.	
IT Human Resource Management	**Needs Improvement**
Processes may exist; however, the lack of maturity has negative effects and needs to be addressed.	
IT Risk Management	**Unsatisfactory**
The combination of process maturity and effect of findings is not acceptable considering the context of the agency, data, or services provided.	
IT Security Management	**Unsatisfactory**
The combination of process maturity and effect of findings is not acceptable considering the context of the agency, data, or services provided.	

RECOMMENDATIONS:

In this report, we issued the following recommendations:
To the department: 5
To the legislature: 0

(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

E-mail
LADHotline@mt.gov

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

Text
(704) 430-3930

Recommendation #1 (page 4):
Governance, risk assessment, and planning
We recommend DOJ develop internal governance structures to specify how DOJ will ensure IT is delivering value, reducing risks, and reporting on key activities, like IT investments, strategic planning, and internal control.

Department response: **Concur**

Recommendation #2 (page 8):
Management and operational effectiveness
We recommend DOJ adopt a set of industry standards to guide the management processes necessary for IT to operate and support agency strategy. This includes documenting and managing the components of the governance system (people, processes, and communication) and how the management approach aligns with overall IT governance.

Department response: **Concur**

Recommendation #3 (page 12):
Management and operational effectiveness
We recommend DOJ create a structure to document knowledge, share knowledge, and transfer to new staff when turnover occurs. DOJ also needs to plan for upcoming human resource risks with replacing MERLIN.

Department response: **Concur**

Recommendation #4 (page 16):
Governance, risk assessment, and planning
We recommend DOJ assess the full scope of risks within IT and the risks IT decisions and strategies pose to the business to build necessary controls within the agency. This process needs to coordinate and direct security management.

Department response: **Concur**

Recommendation #5 (page 20):
System and information management
We recommend DOJ update security documentation and define security needs to meet agency goals and compliance needs. Systems owned, managed, or used by DOJ should operate securely within DOJ's environment, or DOJ should identify how security will be ensured in other environments.

Department response: **Concur**

Chapter I – Introduction, Scope, and Objectives

Introduction

The Department of Justice (DOJ) is Montana's top law enforcement and legal agency. It maintains public safety, represents the state of Montana in court, registers vehicles, licenses drivers, and more. The Montana Enhanced Registration and Licensing Information Network (MERLIN) system is crucial in supporting all of these functions within the DOJ. MERLIN stores information about Montana citizens and is used by multiple agencies. The data within MERLIN assists with other essential state services, including voter registration address verification and jury pool information; Fish, Wildlife & Park's licensing; and child support services.

MERLIN was implemented in 2009 and has been going through modular upgrades since 2013. In November 2020, MERLIN development was finalized when the final upgrade was incorporated into the system. In 2021, DOJ also indicated there were problems due to the age and lack of functionality in MERLIN. DOJ then prepared to replace MERLIN and formally started the project in June 2022.

Audit Scope and Objectives

Even though MERLIN is being decommissioned over the next five years, general controls ensuring information technology (IT) is operating effectively and efficiently are still necessary. The scope of this audit was focused on the general IT controls in place to support any software application used by the Motor Vehicle Division (MVD). Proper execution of these controls will increase the likelihood for success in the implementation of the new system and continuing operations.

General controls reviewed in this audit included governance and management practices. These practices coordinate to guide what an IT division does to support the agency, mitigate IT risks, and ensure application processing meets users' needs. Controls specific to MERLIN processing or enforced by MERLIN were not reviewed due to more significant general control risks identified during planning. These risks were impacted mostly by leadership changes and by changes to IT governance defined in the Montana Information Technology Act (MITA).

Audit objectives included:

- Determine if DOJ evaluates, directs, and monitors IT governance, benefit delivery, risk, and stakeholder transparency.
- Determine if DOJ aligns, plans, and organizes MERLIN and IT operations to ensure MERLIN delivers value, to optimize human resources, and to manage security and risk.

What We Did

IT compliance audit methodologies are focused on reviewing components of processes to identify how capable they are of meeting intended goals, whether it be compliance or controlling risk. Risks to the agency are identified in planning with fieldwork structured to thoroughly review the processes to control or mitigate risk. 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.
- Assessing how the culture and behavior of staff involved in the control process influence the effectiveness.

As part of the compliance audit, we rate how capable each control process is at meeting its intended goal and reducing risk to the agency.

Table 1
Process Ratings

Green	Well-defined processes are organized and measured for performance
Yellow	Basic activities are performed, defined, organized, and managed
Orange	Some activity occurs, yet not organized or defined
Red	Incomplete or incapable process

Source: Compiled by the Legislative Audit Division.

If multiple processes coordinate to achieve a goal, they are grouped into focus areas. We then rate the focus areas based on the cumulation of process ratings and the level of impact the findings have on the agency.

Criteria Used

State law outlines the responsibilities of all agencies to develop and manage security programs, as well as conduct IT resources in an organized, deliberative, and cost-effective manner. To be successful at implementing these requirements, IT governance and management practices are necessary. For example, investment practices ensure IT is cost-effective, management framework ensures processes are organized, and both governance and management practices ensure IT decisions are deliberative.

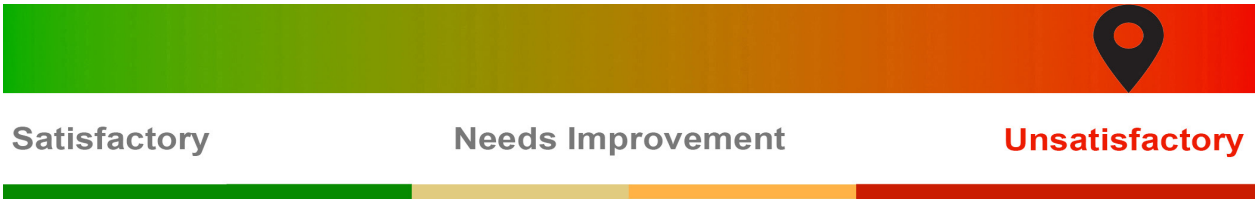
In addition to state law, criteria used for this engagement is based on the Control Objectives for Information and Related Technology (COBIT), which provides guidance on common IT management and governance practices that would ensure state security requirements are met. COBIT domains include IT governance and areas of IT management that:

- Align, plan, and organize IT
- Build, implement, and acquire IT
- Deliver, service, and support IT
- Monitor, evaluate, and assess operations

While DOJ is not required to use this standard, the practices identified are common among private and public sectors. COBIT is a framework of best practices to increase an organization's ability to successfully manage IT and comply with external regulations. COBIT incorporates many industry best practices. These include state required standards, like those published by the National Institute of Standards and Technology (NIST), and the Montana Information Technology Act (MITA).

Chapter II – IT Governance

DOJ has not established IT governance within their organization. DOJ is still building management processes, defining policies, and determining the roles that will support MERLIN. In addition, the department has committed to a replacement system that is being customized and implemented over the next few years. This creates competing priorities and increases risk to the agency.



DOJ needs a structure of IT governance that directs management practices and defines how DOJ information technology investments, benefits, delivery, and risks are monitored, reported, and evaluated in a transparent and regular way.

Importance of IT Governance

IT governance ensures a governing body evaluates strategic options, directs senior management on the chosen strategic options, and monitors the achievement of the strategy. Without IT governance, IT management does not have direction based on agency goals and stakeholder needs, accountability for performance, or guidance for priorities and decision making in line with agency goals or stakeholder needs.

What We Found

Design, evaluate, and update the IT governance structure

DOJ has not articulated IT governance within the agency.

- DOJ intends to participate in statewide IT governance, including state policy. Therefore, analysis did not fully review all governance aspects, like accountability.
- No independent governing entity exists and there is no separation between governance and management.

Ensure value from IT investments, services, and assets

Practices were not in place to provide an understanding of how the value of MERLIN or IT services to MERLIN is measured.

- Performance testing (one aspect of value) was discontinued after key staff left and a vendor was hired to complete.
- No consistent process exists to review the value of systems and determine when significant changes are needed.

Manage risk from an enterprise perspective

DOJ is building a process to review IT risks but had not yet integrated IT risk with the other divisions of the agency.

- The agency was able to discuss risk within MVD and financial risks. The agency also indicated risk was discussed informally in executive meetings.

- There is no formal agency-level process to bring various types of risks together to better understand, analyze, and collaborate on risks or optimize responses to the risks.
- There was no formal plan to address insufficient staffing, system availability, or the impact of a major system replacement to the entire agency. However, the agency has indicated increased risk management activity with the initiation of the MERLIN replacement project.

Engage stakeholders in the IT governance system with transparent reporting

State agencies are required to report to various legislative bodies about IT activity; however, DOJ is now exempt from policy defining how this is done. DOJ has not established what reporting is going forward.

- While DOJ indicated it is going to follow state IT procurement request policy and procedures, DOJ has not defined how or what will be reported to the Department of Administration.
- MERLIN replacement project has been reported to legislative committees, it is not clear how it will be reported to the Legislative Finance Committee.

DOJ has not fully evaluated the organization after changes to the governance structure or established these activities within its organization.

RECOMMENDATION #1

We recommend the Department of Justice develop and implement an internal IT governance framework and seek legislation, where necessary, to specify how the department will integrate with other state IT governance practices including:

A. *Review and approve major IT budget decisions and plans.*

B. *Monitor IT investments, approve IT strategy and reporting, ensure IT aligns with agency strategy, and ensure a structure of internal control exits.*

IT Governance Affects the Success of IT Initiatives and Operations

IT management structure is incomplete, and processes reviewed are not capable of achieving current DOJ goals or requirements. The lack of governance left IT management without direction and support while trying to restructure the division and prepare to replace MERLIN. This had multiple impacts that were identified throughout the entire audit.

Without governance, IT benefit and value are not ensured. Ensuring investments, solutions, and services are effective and efficient requires defining value, determining how performance and value are measured, and monitoring how well the metrics align with agency strategy. It is important for IT to define value targets, measure value, and communicate how initiatives will increase value in specific terms to justify the costs of IT. More importantly, it helps plan for future endeavors, such as system replacements, and sets goals to prevent the same issues from happening again.

IT risks can impact the agency if not managed. Significant risks exist across the business and IT within DOJ, and as IT makes changes, the risk landscape changes. Therefore, it must always be evaluated to direct agency actions in a cohesive, meaningful way. DOJ governance must determine how the systems and activities fit together and where the risk management strategy needs to focus. Otherwise, the likelihood and impacts of risks may exceed DOJ's risk appetite levels.

Stakeholder engagement and reporting is not clear. Identifying stakeholders to engage with the IT governance system and reporting transparent information about IT performance is critical to ensure IT objectives and strategies are align with agency strategy and needs. At this point, it is unclear how, what, and when DOJ communicates with stakeholders of the state IT governance model.

DOJ Hasn't Developed Its Own IT Governance Structure

DOJ was removed from state IT governance model set forth in MITA and has not established its own governance model to coordinate where necessary. During the 2021 Legislative Session, SB 272 excluded DOJ from aspects of MITA, including the governor's ability to require other elective officials to follow DOA IT policies. While some DOJ staff indicated they will still follow state policy, DOJ has not created the internal accountability and enforcement structure that state policy had previously provided. DOJ must define IT governance needs, operational needs, and the level of risk and responsibility for its IT issues.

It is unclear how expertise is shared to advise the governance of IT, information security, and risk. The chief information officer (CIO) of an organization plays a critical role in supporting IT governance. However, the other executive roles are necessary to maintain governance and determine the objectives for the entire agency. DOJ does not have a single traditional CIO role with the technical expertise to advice and validate the IT governance structure. DOJ executive leadership is skilled in operational aspects of management but lacks background and knowledge specific to IT governance structures, processes, work products, and information flows. If bureau chiefs within the JITSD are expected to provide this expertise, the skills, expectations, and mechanism to do so need to be clear within the governance structure.

Chapter III – IT Management

JITSD has faced many changes and challenges and is still in an initial state without a clear management approach for processes, organizational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies. While we identified IT activity occurring, DOJ was still working to establish formal processes and assign responsibilities. The work being completed was dependent on staff identifying what needs to be done, as opposed to a structure that guides staff and establishes expectations.

DOJ needs to adopt a set of industry standards to guide documenting and managing key components (people, processes, and communication) and align them with overall IT governance.

Importance of IT Management Framework

IT management is the administration and monitoring of technology-based activities and resources. IT management systems must clarify important components that make processes consistent and understood, such as process steps, roles and responsibilities, and communications. Agencies must create a consistent management approach to meet state governance requirements, such as security or public reporting. DOJ must have a robust IT management framework to meet agency responsibilities to citizens and the federal government.

What We Found

Design the management system of roles, processes, policies, skills and competencies

Key management policies and procedures have not been defined (IT risk, security, and strategy).

- Roles and responsibilities are not clear or complete and the organizational structure changed multiple times during fieldwork.
- DOJ indicated progress was being made towards formalizing and identifying missing policies and procedures.

Implement management processes, organizational structures, infrastructure, services, and applications to support the management system

Multiple activities occurred in separate areas that were not managed in a way to ensure they were repeated and reliable.

- JITSD adjusted the organizational structure multiple times as staff departed.
- MVD filled more roles related to IT, such as data conversion, areas of project management, system maintenance, and IT architecture as employees left JITSD.

Evaluate and update the management framework

Policies, procedures, and information are not complete or maintained (business continuity, system security plans).

- As staff left, key responsibilities were not officially reassigned (disaster recovery programs, risk assessments, and mitigation planning). We found evidence of the previous administration's management practices that current staff were not aware of.

DOJ's IT management structure consists of some necessary activities but is not complete or comprehensive.

RECOMMENDATION #2

We recommend the Department of Justice improve the IT management system by:

A. *Selecting industry standards that guide what management processes and components should be in place and how to evaluate them for effectiveness and efficiency.*

B. *Document the components of the management framework, including policies, procedures, communications, organizational structures, roles, responsibilities, and other necessary components to achieve the goals of the agency and IT.*

C. *Define the communication structure of the management processes and roles and how they will interact with IT governance.*

Management Frameworks Are Critical for Processes to Be Effective

Success in areas of IT is unlikely and not repeatable. Management structures benefit organizations by allowing processes to be easily repeatable. This is a critical step toward growing in maturity and moving forward to where processes can be optimized (reviewed, measured, and improved strategically). Planning a process includes documenting it so that awareness is created, and in case staffing changes occur, the process can remain the same. Otherwise, processes become reliant on the people in the positions that happen to know what to do. Change becomes reactionary, and knowledge transfer of the process becomes a challenge.

Maintaining controls during turnover becomes more difficult. DOJ lost knowledgeable staff that were essential for MERLIN and IT operations. DOJ struggled to recruit staff throughout the end of 2021. In a situation where staffing is not adequate, management systems help identify the necessary skills and competencies needed for internal development or external recruiting. This ensures critical processes and controls will not be weakened by staff leaving. The effect of staff turnover is also compounded when agencies rely on staff to maintain operations instead of a management structure that supports and guides staff.

DOJ Is Still Formalizing the IT Management Framework

DOJ struggled to identify the previous IT management framework. DOJ indicated challenges in understanding the IT management framework after leadership changes. We were able to find evidence of the basis for IT management practices in the previous administrations' files. However, DOJ staff stated that the documents and evidence weren't formally adopted by the previous administrations. These challenges led to DOJ deciding to update IT policies, procedures, and roles to align with a modern governance framework.

Unclear how expertise is shared to update the IT management framework. The JITSD administrator was brought in to administer the division, while the bureau chiefs used their technical knowledge in a supporting role. If this is the case, there needs to be a clear structure of how these individuals work together to make informed decisions and how the technically-knowledgeable staff are involved in determining the IT management framework. Choosing a set of industry standards that best fit DOJ would provide guidance on what processes and coordination are necessary to achieve goals.

Chapter IV – IT Human Resource Management

JITSD has experienced high turnover that created knowledge gaps relative to MERLIN. Identification of key IT personnel and practices to maintain critical processes were not utilized during leadership changes and over the course of 2021 when staff turnover was high.

While the division rebuilds staffing resources, it needs to include a structure to knowledge capture (documentation), knowledge sharing, succession planning, staff backup, cross-training, and job rotation initiatives to minimize reliance on a single individual performing a critical job function.

Importance of Managing Human Resources Within IT

Agencies optimize human resources capabilities by providing a structured approach to ensure optimal recruitment/acquisition, planning, evaluation, and development of human resources (both internal and external). To provide necessary citizen services and meet agency goals, DOJ needs competent and motivated staff with a mutual understanding of MERLIN technology and business knowledge, expertise, and initiatives for business innovation.

What We Found

Maintain adequate, skilled staff

Staffing levels were low in the second half of 2021 while DOJ was trying to balance maintaining MERLIN with replacing it.

- JITSD turnover was significant in 2021 (41 percent attrition rate, 19 staff left) and previous contracted support staff were terminated in June 2021.
- DOJ was able to use flexible staffing arrangements, such as the three exigent developers hired to work up to 3,696 hours between December 2021 to June 2022 at $130/hour.

Identify key personnel

JITSD has no structure for knowledge capture and transfer and new staff coming into key roles were not given necessary information.

- After August of 2021, DOJ was solely dependent on a single developer with MERLIN knowledge that was working part-time at DOJ while working full-time for another agency.
- MVD is building a structure for knowledge capture and transfer.

Assess and manage performance

DOJ HR provides structured processes to annually assess performance using enterprise and department objectives, goals, etc.

- Basic human resources (HR) practices exist on a individual basis, however, it was not clear how future activities are impacted by goal setting, succession planning, and career development processes.

- JITSD discussed improving how they are able to reward employees as part of improving retention.

Maintain skills and competencies

Training activities are more developed in MVD than in JITSD.

- DOJ has developed specific MERLIN training for business staff and MVD has robust training materials for new MVD staff.
- Training for MERLIN-related IT is on-the-job training and coaching from a part-time former developer.
- Succession planning for key individuals was not fully considered and large knowledge and skill gaps were created in JITSD.

Plan and track resources

The agency committed to staffing MERLIN at all costs but was not able to articulate what the plan is to move forward from the current, understaffed situation.

- DOJ HR creates yearly reports on the usage of IT and business human resources for the entire agency.
- We were not able to identify a clear, feasible staffing plan for MERLIN over the course of transitioning to a new system.

DOJ does not have a consistent structure for knowledge capture and transfer or plan for changes in key IT positions.

RECOMMENDATION #3

We recommend that the Department of Justice:

A. *Develop the structure of knowledge capture and transfer that reduces reliance on a single individual to manage critical processes.*

B. *Formalize the analysis and plan to mitigate the immediate human resource risks of maintaining MERLIN through the transition to the new system.*

Turnover and Knowledge Gaps Have Affected DOJ's Progress and Increases Risks

MERLIN staffing issues affected the transition to maintenance status. In September 2021, DOJ did not have adequate staff for maintenance of MERLIN. During this time, MERLIN fixes were limited as DOJ tried to stabilize the system. MVD and JITSD staffing had to adjust and adapt as the responsibilities of staff that developed the product shifted to support staff that were going to troubleshoot, enhance, and maintain the product. There is a lot of risk involved in this process, and key practices need to happen, such as knowledge transfer, communication, and service agreement. Success of the system can be delayed, and users can become frustrated to the point of rejecting the system.

DOJ was able to establish flexible resource arrangements with staff augmentation and part-time work. DOJ had to adapt their staffing plans after the last MERLIN developer departed in 2021. DOJ hired three exigent staff with experience in MVD application solutions and created an agreement to split the last developers' time between both DOJ and the new job. The part-time developer was required to onboard the contracted staff and transfer knowledge. While this improved staffing for MERLIN, DOJ is relying on the part-time developer to lead onboarding and training of the three exigent staff, as apposed to a structure of knowledge capture and organized knowledge transfer.

The business is hiring additional staff with IT-related responsibilities. While MVD has consistently employed MERLIN support staff, MVD added more IT-related roles during the staffing problems JITSD was experiencing and to prepare for system replacement. Within MVD, an IT manager has been hired with the same core competencies and responsibilities as the IT managers in JITSD. This section of MVD has also taken on some of the IT service responsibilities specific to MERLIN and replacing MERLIN. Areas of data conversion, project management, quality assurance, IT architect and support all exist within MVD on this team. This creates a decentralized structure for IT practices and requires much more coordination and oversight within an agency.

MERLIN is at risk of disruptions/impacts during the transition to a new system. Though JITSD has staff for managing maintenance, recovery operations, and performing recovery testing, the expertise needed to inform those efforts is at MVD. MVD is thinly staffed for testing MERLIN releases, and staffing for an emergency will be difficult for DOJ. The system replacement effort can also put staffing levels at risk due to changing priorities.

DOJ Over-Relied on Staff Without Preparing for the Effects of a Major System Replacement

DOJ depends on staff to do necessary work without a structure in place to guide and ensure effectiveness and efficiency. DOJ has not assigned responsibilities of key IT practices to IT staff or identified gaps in employee classifications and practical work. The current administration did not have a plan to understand the current environment and adjust to staffing changes, nor did it have a plan that would ensure specific, critical processes would be identified and maintained. DOJ is relying on talented individuals to maintain practices instead of creating a structure where roles and responsibilities are clear (what) and critical processes are covered by knowledgeable and capable (how) staff.

DOJ is focused on long-term goals, without formally planning for immediate risks. While DOJ was able to react with flexible staffing arrangements, a formal process to manage the risks of staff leaving was not in place. A formal risk management process may have better prepared DOJ for turnover and reduced knowledge gaps. For instance, DOJ identified issues with culture and morale during leadership changes, both being indicators of staffing risks and key focus areas when organizations undergo change. Early analysis of the strategy and messaging to replace MERLIN needed to include the impact on turnover, key assets or practices that need to be maintained, and safeguards intended to mitigate control weaknesses during turnover. This may have prepared DOJ with better strategy to respond to HR risks. In the future, DOJ will be better able to ensure the control structure is maintained when turnover or organizational changes occur.

Chapter V – IT Risk Management

Information Technology risks related to MERLIN are not formally managed. While we identified individual risk activities, DOJ is still developing a process to continually identify, assess, reduce, and report IT-related risk, especially MERLIN risk, within tolerance levels set by agency executive management. DOJ is still developing a process to make risk quantitative, gather information to analyze risk, and make risk relative for comparison, prioritization, and appropriate response.

DOJ needs to assess the full scope of risks within IT and the risks IT decisions and strategies pose to the business to build necessary controls within the agency. This process needs to coordinate and direct security management.

Importance of IT Risk Management

IT risk consists of threats to data, systems, processes supported by systems, as well as the threats IT decisions have on agency goals. Agencies need to continually identify, assess, and reduce IT-related risk within tolerance levels set by agency executive management. Information systems like MERLIN have multiple dependencies and partners within DOJ. MERLIN, like all DOJ systems, needs to be a part of the DOJ agency IT risk management framework.

What We Found

Collect data

Data collection is not systematic or directed from a managed process.

- Data is collected in silos, specific to individual areas, and not formally aggregated (project risk, cybersecurity risk, financial risk).
- We did not identify an inventory of known risks, risk attributes, control activities, or analysis (recovery, continuity, security, compliance, personnel, etc.).

Analyze and articulate risk

Risk is not analyzed in terms of likelihood and impact, quantified, validated prior to decision-making, or reviewed for optimal risk response.

- Informal discussions about risk occur, but are lacking mature data collection to be able to support comprehensive analysis.
- Risks were analyzed by a vendor as part of replacing MERLIN, and DOJ indicated that replacement project risks are managed by the agency and vendors involved. However, internal processes to manage risk for all of IT and MERLIN through transition are still being developed.

Create a treatment plan and respond to risk

Risk response is not formal and becomes reactionary after impacts are realized (personnel risks, knowledge transfer, compliance).

- Response plans for MERLIN system were out-of-date and have not been tested.
- DOJ shares risk response with other entities (vendors and the State Information Technology Services Division); however, agreements are out-of-date and updates are still in progress.

DOJ is still developing a comprehensive management structure for mitigating IT risk or using comprehensive risk analysis to drive strategic decisions.

RECOMMENDATION #4

We recommend the Department of Justice:

A. *Adopt a risk management framework to guide the development of enterprise risk management,*

B. *Develop the IT risk management process in line with DOJ risk appetite and within risk tolerance levels,*

C. *Establish risk metrics to inform decision making, and*

D. *Identify and assign risk management procedures for necessary individuals through policy or position descriptions.*

Risk Management Affects the Success of IT Initiatives and Helps Prioritize IT Improvements

MERLIN is at risk of major interruptions. Any major system replacement changes the risk landscape for an agency. Formal approaches to risk management bring awareness, coordination, and expectations throughout the entire agency. Within DOJ, data on these risks are not being gathered to understand and communicate them throughout the entire enterprise in a consistent, formal manner. Project risks are being managed by multiple vendors and DOJ. The analysis and prioritization of these risks must be coordinated between the replacement projects, compliance, and other identified IT risks. DOJ indicated it is establishing proper committees and communication to further develop risk management at an enterprise level. Without this coordination, determining the priority of project risks and current operations may lack justification and guidance.

Improvements will increase the success of the replacement project. While the IT manager's role in MVD is to review project risks in coordination with vendors, this isn't enough to protect the project completely. As a project initially estimated to cost over $60 million, risks must be minimized. Risks must be communicated through the organization and addressed as a team to ensure support from various divisions involved. This is especially critical in DOJ's situations where IT roles exist in both MVD and JITSD.

JITSD needs to focus limited resources in the highest risk areas. Risk management helps provide priority and direction in completing initiatives. As JITSD has drafted many initiatives and is working to rebuild the division, proper risk management is needed to ensure the available resources are being focused on the right tasks. High priority risks are competing for resources, such as incident response, business continuity, major IT project reporting, and some of the policies recommended by this audit.

The agency may over-rely on others to manage risk and not fully consider all risk in decision making. Risk management is the responsibility of the agency and crucial when making changes to transform and modernize operations and technology. Transitioning to cloud solutions is an example. Cloud solutions do not eliminate risk or transfer the responsibility entirely to a vendor. The risk landscape changes, and the agency still must ensure the vendor is held accountable to contractual agreements and security standards.

Risk Management Is Not Fully Developed

DOJ has not formally assigned risk management responsibilities through position descriptions or policy. DOJ does not have management responsibilities that would encompass agency risk management or IT risk management present in job descriptions. DOJ indicated that the JITSD administrator has the responsibilities of the IT executive classification, even though the position is personal staff and does not have a formal position description. This classification only outlines the responsibility of making decisions about risk strategies, not formally managing it. This and the lack of policy defining risk management leaves no one formally responsible for risk management within JITSD or for agency risk management within DOJ.

DOJ worked towards meeting standards; however, still lacked direction for establishing enterprise-wide risk management. The lack of governance and risk management direction means that DOJ does not determine what risks to focus on (risk appetite and tolerance), how to measure risk (risk metrics), or who manages risks. While DOJ has addressed various standards related to risk management, DOJ has not adopted or referred to a framework that guides the entire agency in establishing those aspects of risk management. This type of framework is necessary to ensure responsibilities are assigned and understood by everyone involved across multiple divisions of DOJ.

Chapter VI – IT Security Management

Security practices are taking place; however, DOJ is still transitioning to managing security at an enterprise level. DOJ has some components that constitute a security-oriented posture, such as incident detection and response. However, what exists is still in an initial state because the components and entities involved are not integrated and clearly accountable for the full scope of the program.

Satisfactory | Needs Improvement | Unsatisfactory

DOJ needs to update security documentation and define what security needs to be to meet agency goals and compliance needs. Systems that are owned, managed, or used by DOJ should be authorized to operate securely within DOJ's environment, and DOJ should identify how security will be ensured from a risk and compliance perspective in other environments.

Importance of IT Security Management

Due to the sensitive information within MERLIN, DOJ must comply with federal requirements to be able to share criminal data. DOJ must also have a comprehensive security program of its own to reduce risks not associated with federal compliance, such as Montana's own security requirements. While DOJ is not under the governance of SITSD, it is still part of the statewide network and needs to maintain security at or above minimum requirements to not only protect its information but to protect the statewide network and other agencies.

What We Found

Establish and maintain the security management system

DOJ is in process of rebuilding, training, and coordinating security management activities and responsibilities.

- The scope and boundaries are not internally defined and relationship with SITSD is not clear, causing confusion while trying to document security controls.
- The overall approach appears to be compliance-based and reactionary to external needs without direction from a formal risk management process.

Define a security risk treatment

System security plans were incomplete and out-of-date.

- Available diagrams are out-of-date and documentation is incomplete.
- The security team's first priority was establishing cyber incident monitoring, response, and reporting through executive dashboards.

Monitor and review the security management system

Auditors identified some policies and the overarching information security policy defining an information security management system. However, these documents are still in the process of being updated by DOJ.

- There were no plans for internal review of security management procedures.

DOJ is still developing security management processes to coordinate the security activities occurring and to understand the overall security posture of MERLIN and IT in general.

RECOMMENDATION #5

We recommend the Department of Justice improve security management by:

A. *Updating the information security policy with scope and security management responsibilities,*

B. *Clearly defining the responsibilities and ownership of controls within DOJ and those shared with SITSD,*

C. *Ensuring the security program is integrated into the risk management process, and*

D. *Formalize the process that enforces minimum state security standards for applications/systems/activities before they are authorized to operate on or access the state network.*

Enterprise Security Management Affects the Security Posture of DOJ and Strength of Internal Controls

DOJ is at risk of noncompliance with federal requirements. Due to the criminal justice information and personal information managed by MERLIN and other systems within DOJ, a high level of security is required for DOJ to be able to interact with federal partners and ensure the confidentiality and integrity of that information. If DOJ were to not comply with these requirements, there could be exclusion from federal programs and grants and potential fines.

Security controls may lack oversight and enforcement. Without an overarching enterprise security program, related controls, such as application controls, can be changed, disregarded, or ineffective as time goes on. A formal process to review and monitor controls needs to occur regularly and as changes are made, such as changes to MERLIN from system issues and the system replacement.

Security can become externally driven by compliance instead of internally planned to meet business and agency needs. A compliance mindset in security may not align with all business and agency security needs. Compliance is focused on the needs of an external entity, which may not consider the agency's specific environment. Compliance is often a minimum standard that may not be enough to reduce risk to an acceptable level within the agency. Therefore, it's important to decide internally what the security program needs to be. This will reduce the risks specific to the agency environment as well as meet compliance requirements.

DOJ Is Still Rebuilding the Security Program

Security policy defining the scope of the security program has not been updated. We identified a security management policy with an effective date of 2011 and no revised date; however, it showed a modified date of December 2020. This document did not appear to be formally adopted by DOJ. No other documents define the scope of the current security program, basic high-level procedures required in the security program, or the roles and responsibilities of all staff involved in the security controls. The scope of security management, outlined in a security management policy, was not comprehensive for an enterprise-level security program.

Knowledge transfer during security staff turnover impacted new staff's ability to update formal security management processes. The security team of the DOJ completely turned over during 2021. Starting in October 2021, DOJ began to rebuild the team. Current security staff indicated minimal information was shared or given to them when they started their jobs. Current staff indicated they were developing the MERLIN security plan that was not yet complete or in place. While we were not able to assess the full extent of the security program prior to the turnover in security staff, auditors were able to identify older versions of some security documents and were informed by previous staff that formal documentation existed prior to the new security team being established. DOJ did not initially plan to identify and build from or update these documents. The team developed specific areas of cybersecurity first including:

- External threats (incident tracking and response),
- Internal architecture (the design and placement of security controls and tools), and
- Enterprise application security (access management).

Turnover of security team created responsibility gaps. While the security team is now developing security management to coordinate these areas with other areas of JITSD and MVD, DOJ does not have a single person formally responsible for the security management system. Previously, DOJ had a security supervisor formally responsible for key activities, like disaster recovery and risk assessment. DOJ indicated that in the new structure, one of the security specialists would take a "lead" role and have additional responsibilities related to security policy and compliance with external audits. This still leaves the formal responsibility, along with necessary skills and competencies that build accountability, missing within JITSD's IT operations.

Department of Justice

Department Response

AUSTIN KNUDSEN

STATE OF MONTANA

September 13, 2022

Legislative Audit Division
Attn: Director Angus Maciver
1301 E 6th Ave
Helena, MT 59601

RECEIVED
September 13, 2022
LEGISLATIVE AUDIT DIV.

Dear Director Maciver,

The Department would like to thank the Legislative Audit Division staff for their dedication to this audit. Early in this administration, the Department recognized that many documents were incomplete or not transferred as part of the transition, making the jobs of the Legislative Audit Division and the Department more difficult. The Department would have benefited from this thorough process earlier in 2021.

You and your staff have the respect and appreciation of the Department. The Department believes that identifying the best practices of various IT governing agencies will provide the best guidance and improve the Department's abilities to serve Montana citizens.

Sincerely

Austin Knudsen
Attorney General

DEPARTMENT OF JUSTICE

215 North Sanders
PO Box 201401
Helena, MT 59620-1401

(406) 444-2026
Contactdoj@mt.gov
mtdoj.gov

Recommendation #1

The Department of Justice ("The Department") concurs and has been implementing an IT governance structure that complements the State's while also accounting for Montana Information Technology Act (MITA), National Institute of Standards and Technology (NIST), and Criminal Justice Information Services (CJIS). The Department plans to continue the Information Technology Procurement Request policy that reports to Legislative Finance Committee (LFC) any major procurement, allowing for review and approval via the legislative process. Furthermore, we concur that monitoring investments, approving strategy, and reporting are vital tasks that have functioned well under the Department in working with the legislature.

The Department has formed a leadership group including executive, IT, and central services staff and stakeholders that will review and implement a full IT governance and management structure that considers each of our divisions' unique needs and considerations. The Department will continue working to effectively communicate that structure to all leadership and staff.

Recommendation #2

We concur that the Department will continue to improve the IT management system. The Department has identified an industry standard, NIST for Cybersecurity, that guides the day-to-day and long-term operations for the IT needs of the Department. The management framework reflects the NIST standards, which are commonly adopted by law enforcement agencies and state governments. Additionally, the Administrator will further develop the communication of the structure and managements process and roles to reflect the identified NIST standards and others identified to fulfill the needs of the Department.
As explained in our response to recommendation #1, the Department has formed a committee with each division/stakeholder to better inform the Department's IT needs to meet our mission and goals.

Recommendation #3

We concur that knowledge capture is vital in any transition. The Department, via management and human resources, works to provide a high level of knowledge transfer via both formal and informal meetings with the departing employee. (This includes a formal exit interview.) Department leadership recognized the dependence on single employees for operations early last year and implemented cross training to reduce isolation of system knowledge and improve transitions. That process is now in place and managed by the Department's software manager and Business Bureau chief.

The Department completed a risk assessment of human resources, which lead to the restructuring of MERLIN updates to a more staged and controlled environment and allowed for the former lead developer to provide oversight, implementation, and trainings for new employees. In December 2021, the Department took the additional step of retaining three exigent developers with extensive knowledge of MVD-type systems. These contracted employees work on an as-needed basis providing a high level of support, while greatly reducing the overall cost of maintaining the system.

Recommendation #4

The Department concurs with this recommendation. The Department has identified NIST as the best model framework to develop and adapt for the needs of the agency. Currently IT risk is discussed between IT and seven divisions of the Department. The Department is working towards a more mature process and is forming an IT Risk Assessment Board (IRAB) to review, understand, and address risks across the agency. The Department's current practice is to follow the NIST risk assessment guidelines and, through an IRAB working group will identify and implement the NIST policies that address the agency's needs to manage risk and comply with applicable statutes and Montana Operating Manual policies.

Recommendation #5

The Department concurs with the recommendation. The Department will continue to update security polices and management responsibilities to reflect NIST standards. The Department has an Information Security Officer who is leading a team to fully update and develop policies that meet our needs, goals and mission. The Department, through its leadership and human resources teams, has defined the roles and responsibilities of staff within the Justice IT Services Division (JITSD). The leadership of JITSD is updating the memorandum of understanding between the Department and Department of Administration's State Information Technology Services Division to clearly define ownership of the activities and needs of both parties.

The Department's Information Security Officer, JITSD Administrator, and IRAB will work to build policies, procedures, and practices to integrate the risk management needs of the Department with the IT security needs. The Department's Security Team, IT Help Desk, and all JITSD employees understand the necessity of a secure network. Department staff will formalize the existing practices and procedures to a format in line with the recommendations of the Legislative Audit Division (LAD).