LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller
Miki Cestnik

Memorandum

TO: Legislative Audit Committee Members

FROM: Tyler J. Julian, Associate Information Technology Auditor

CC: Department of Justice
Austin Knudsen, Attorney General
Will Selph, Chief of Staff
Stephanie Cote, Administrator, Central Services Division
Missy McLarnon, Chief Information Officer, Justice Information Technology Services
Lauri Bakri, Administrator, Motor Vehicle Division

DATE: August 2024

RE: Information Technology Audit Follow-Up (24SP-10): *The Montana Enhanced Registration and Licensing Information Network (MERLIN)* (orig. 21DP-01)

Introduction

We issued the *The Montana Enhanced Registration and Licensing Information Network (MERLIN)* (21DP-01) report to the Legislative Audit Committee in October 2022. The audit included five recommendations to the Department of Justice (DOJ). In March of 2024, we started follow-up work to assess implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

The Department of Justice oversees the Montana Enhanced Registration and Licensing Information Network (MERLIN), used for the state's vehicle and title registration and driver-licensing services. Our audit examined the DOJ's IT governance and IT management practices as they apply to MERLIN. We found the DOJ's lack of structure for IT governance limits the department's ability to support agency goals, provide services, and meet requirements, which puts the MERLIN replacement project at risk of encountering issues and not meeting goals. In response, the department has established responsibilities for governance and started working on an overall IT management framework and security policy. The audit contained five recommendations, one implemented and four being implemented.

Background

The MERLIN system is administered by the Motor Vehicle Division (MVD) of the Montana Department of Justice. MERLIN is a large and complex system incorporating multiple functions such as vehicle title and registration, financial and accounting processes, and dealer and driver licensing to manage MVD's business processes. During the audit planning , the DOJ made the decision to replace MERLIN. Therefore, the scope of the original audit was to assess DOJ general controls as they apply to MERLIN and future IT systems and operations. How about: During audit planning, the DOJ decided to replace MERLIN. Thus, the original audit assessed the DOJ's general controls for MERLIN and future IT systems.

Many issues identified were attributed to informal IT governance and IT management at the agency level. During the audit, we found that high turnover created knowledge gaps relative to MERLIN, and identifying key IT personnel and practices to maintain critical processes during replacement were not utilized. We found that IT risk is not formally managed to continually identify, assess, reduce, and report IT-related risk within agency tolerances. We also found that while day-to-day security practices at DOJ are taking place, DOJ has not yet fully established practices to manage security at the enterprise level.

Our original audit of MERLIN resulted in five recommendations to the department, all of which were met with concurrence. These recommendations were made to address IT governance and management issues.

Audit Follow-up Results

During the follow-up, we worked with Justice Information Technology Services (JITS) to understand DOJ's efforts to develop internal governance structures designed to ensure IT is delivering value, reducing risks, and reporting on key activities. We interviewed DOJ staff responsible for IT governance and management, reviewed supporting documentation, and examined the boards created to advance the implementation of recommendations.

After the audit, DOJ experienced management turnover. However, the department has made progress on the audit recommendations. The following sections discuss our recommendations and detail the department's progress toward their implementation.

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.

Implementation Status – Being Implemented

The audit found that DOJ had not established IT governance within their organization. After being exempted from aspects of state IT governance outlined in the Montana Information Technology Act (MITA), DOJ was still building management processes, defining policies, and determining the roles for overall effective IT governance.

This recommendation intends that DOJ implement an IT governance framework and a governing body to reduce the likeliness of risks and losses related to the management of data, technology, and business operations. IT governance formalizes the standards and processes to ensure that IT investments are necessary, feasible, and deliver intended results.

Since the audit, the DOJ has created the IT Steering Committee that acts as a central advisory and coordinates DOJ divisions' business processes driven by technology. This committee discusses long-term IT planning, potential risks, the IT needs of each division, and the prioritization of projects and IT resources. This group is also responsible for for reviewing and finalizing major IT budget decisions, policies, and division and department IT plans.

DOJ has also created the DOJ IT Policy Board (ITPB) to provide governance for decision-making when addressing the IT functions of the DOJ and the systems and agencies they support. DOJ intends to follow State IT policy; however, the ITPB was created to account for DOJ-specific requirements and exemptions from State policy. The ITPB develops and enforces DOJ IT policies and is collaborating with the Department of Administration (DOA) to ensure that division IT plans, and the DOJ IT plan is completed and reported to the DOA for the statewide strategic IT plan.

While the structure DOJ has created addresses aspects of both A and B of the recommendation, further work by the ITPB and Steering Committee is necessary to clearly outline how DOJ will address areas of the State's governance requirements from which they are exempt. DOJ needs to develop procedures and criteria to inform consistent and repeatable decision-making, including:

- The criteria necessary for the approving major IT budget decisions and plans.
- Procedures and metrics for monitoring IT investments.
- A procedure to ensure a structure of internal control exists prior to authorizing a system's operation.

DOJ expressed that they have commonly established criteria and ad hoc procedures to guide decision-making and determine whether a system will be authorized to operate. DOJ intends to formalize these items as part of its governance by the end of the first quarter of 2025.

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.

Implementation Status – Being Implemented
The audit found that DOJ lacked clear procedures to guide effective IT management. Key management policies and procedures were not identified or defined, and existing policies and procedures were incomplete or not maintained. As the organizational structure changed, key roles and responsibilities were not reassigned, and several necessary IT management activities were not performed in a repeatable and reliable manner.

This recommendation intends for the DOJ to develop an IT management framework and document its components to meet agency responsibilities to citizens and the federal government. Choosing an existing IT management framework based on industry standards saves effort, provides best practice guidelines, supports knowledge sharing, and aids future control assessments.

Since the audit, DOJ has created an IT framework planning and security policy. While this is evidence of DOJ's effort and progress toward implementing the recommendation, the current framework emphasizes what requirements shall be met. It does not yet include other components necessary to operationalize tasks required to meet requirements. DOJ still needs to create key policies and procedures to support the framework. This provides clear guidance on meeting requirements, timing, responsibilities, and communication of results to support aspects of governance and management.

A focus on meeting requirements without defined processes and responsibility for ensuring the completion of specific processes puts the DOJ at risk of being reactive and adopting ad hoc IT management procedures. Developing a comprehensive IT management framework and documenting the multiple necessary components is a substantial task. The DOJ is committed to developing a comprehensive IT management framework but has not given a timeline because of the extensive work required.

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.

Implementation Status – Implemented
The audit found that the high turnover experienced within DOJ in 2021 created knowledge gaps in both JITS and MERLIN, and the identification of key IT personnel and practices to maintain critical processes were not effectively utilized. This led to new staff being unsure or unaware of their duties and the need for additional staffing arrangements to accomplish the work necessary to continue operations.

DOJ needs a structured approach to manage human resources to meet agency goals and successfully provide necessary citizen services. Managed human resources ensures adequate talent acquisition, planning, evaluation, and the development of these personnel. This structure should include knowledge capture, sharing, staff backup, cross-training, and job rotation to reduce reliance on any single individual for critical functions.

Since the audit, JITS has implemented the means to minimize reliance on a single individual performing a critical job function.

- JITS has successfully implemented a system to serve as a knowledge repository for IT documentation and to facilitate project management. While still in the early stages of adoption, the intention is to use this system to document the DOJ IT policies and procedures that are being developed, communicate and report on different aspects of IT management, and track and manage the status of different JITS managed projects going forward.

- DOJ has also identified the roles and allocated additional human resources necessary to support the MERLIN replacement. Two MVD personnel are directly responsible for the maintenance of MERLIN during the transition (along with other MVD staff familiar with MERLIN data), and three JITS personnel assist with both the maintenance of MERLIN and conversion of MERLIN data during transition. This cross-training and sharing the responsibility for MERLIN maintenance between multiple staff reduces the reliance on a single individual to maintain MERLIN during the transition.

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.

Implementation Status – Being Implemented
The audit found that the DOJ does not have a formal IT risk management process. While the DOJ performs some risk management activities, the collection of risk-related data is not systematic and risk is not appropriately analyzed regarding risk appetite or tolerance. As such, DOJ's risk response is also not formal and becomes reactionary after impacts are realized.

Since the audit, the DOJ has outlined an IT risk management framework as part of its overall IT management framework and added risk assessment to the procurement process. DOJ has an IT Request Review group that performs risk assessments for newly proposed hardware and software and provides recommendations to the Steering Committee to be considered during approval. However, the DOJ has not yet developed the policies and procedures or assigned the responsibilities necessary to enable effective IT risk management in other areas. Ongoing efforts are crucial because effective IT risk management ensures compliance, improves planning and IT initiative success (e.g., MERLIN replacement), and provides essential information for informed decision-making and task prioritization.

DOJ is progressing towards implementing the recommendation and indicated they intend to continue the development of their IT risk management practices after the replacement of MERLIN is complete in 2025.

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.

Implementation Status – Being Implemented
The audit found that the DOJ performs necessary IT security practices, but its IT security management program is incomplete. The program is compliance-based to meet external needs without direction from a formal risk management process. Various aspects of the security program needed improvement and further clarification, such as system security plans and the scope and boundaries of the security program. DOJ's relationship with SITSD was unclear, causing confusion when documenting responsibilities for security controls.

Since the audit, the DOJ has started work on its information security policy, which, includes scope and security management responsibilities. The overall responsibility for security management is assigned to

JITS policy owners, that can delegate responsibility at their discretion. While this is an improvement, further development of specific policies and procedures to define responsibility and ensure the execution and enforcement of the information security policy is required.

DOJ is at varying stages of implementation for parts B, C, and D of this recommendation:

- The DOJ is working with SITSD to better understand its relationship and how it impacts security responsibilities with regard to shared control ownership. These conversations were in the initial stages at the time of follow-up.
- DOJ risk management is currently limited to product evaluation at the time of proposal, without on-going risk analysis from a broader IT or enterprise approach or perspective.
- DOJ still performs an informal process to authorize applications/systems/activities to operate on the state network. However, authorizations occur without a recurring risk or control assessment as the basis of the decision.

The DOJ stated it has plans to continue this work. However, formalizing security management practices to implement this recommendation will require further progress toward DOJ's IT risk management practices.