LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Joe Murray, Deputy Legislative Auditor
Performance and Information Systems Audits

DATE: January 2020

RE: Potential Information Systems Audit Areas for Calendar Year 2020

Please find enclosed a list of potential information systems audit topics for calendar year 2020. This list has been compiled to provide an opportunity for the Legislative Audit Committee to highlight areas of interest for future audit work. These topics have been identified through previous audit work, areas of legislative or general interest, and initial review of the value and risk of state agencies' systems or applications.

Potential audit topics include:

- Fish, Wildlife and Parks (FWP) Licensing & Reservation System (Explore MT)
- Public Defender Case Management System
- eGovernment Services in Montana
- State of Montana Benefit Plan Eligibility and Administration System

We are requesting you assign a priority ranking (low, medium, high, or very high) for the potential topics on the attached list. It is important you assign a score to each topic; any unassigned score will result in a low priority score being applied to that specific topic.

To assist in scheduling information systems audit work for the next year, we would like to receive your priority rankings by January 17, 2020, if possible. If you are unable to turn in your prioritization rankings by that time, you may also return them to the office by mail, fax, or email. We will be available during the committee meeting and legislative week for any questions or comments regarding the potential information systems audit list.

Enclosure

S:\Admin\Correspondence\20\LAC\January\jm-LAC-IS-prior-memo.docx\cr

Room 160 · State Capitol Building · P.O. Box 201705 · Helena, MT · 59620-1705
Phone (406) 444-3122 · FAX (406) 444-9784 · E-Mail lad@mt.gov
https://leg.mt.gov/lad

Rvwd By: ah
Mailing Status: hd
Date: 1/14/20
ECS sent: cr

Information Systems Audit
CY2019 Topic Update

Audit Topic Updates:

Agency	Audit Topic	2019 Average Score
Secretary of State	Montana Voting Systems	3.6
Update: Audit in progress.		
Montana University System	Banner Data Security Across the Montana University System	2.6
Update: Anticipated start in spring 2020.		
Department of Public Health and Human Services	Marijuana Enforcement Tracking Reporting Compliance (METRC)	2.6
Update: Removed from high-priority list due to legislative changes in last session and recent system changes.		
Department of Administration	State of Montana Data Centers	1.9
Update: Reviewing assurance needed for data centers as an ongoing, biennial project.		
Department of Justice	Montana Enhanced Registration and Licensing Information Network (MERLIN)	1.8
Update: Removing from high-priority list due to three consecutive years of low interest and priority.		

Audit Topic Descriptions:

Fish, Wildlife and Parks (FWP) Licensing & Reservation System (Explore MT)

Explore MT will replace the current FWP Automated Licensing System (ALS). Explore MT will provide over 68 types of resident and commercial licenses, as well a reservation system for campsites and amenities. Licenses and associated fees make up approximately 65 percent of FWP's $95 million operating budget. The 2019 legislature approved $10 million of HB10 money for its development. At this time, FWP is evaluating contractor responses to its recent bid proposal which closed on January 8th. The bid consists of 1,966 requirements and has 193 attachments related to core business areas: licensing, lottery/draws, reservations, and the accounting of all funds generated by the business processes. FWP states the system will integrate software and hardware to conduct current business processes on a modern technology platform that provides process efficiencies, system maintainability, and expanded functionality. FWP notes it is of the utmost importance that the integrity of customer data be faultlessly maintained throughout the project. Audit topics could include: validating risk and risk mitigation plans, validating project requirement, assessing feasibility of project and funding plans, verifying work is successfully completed, and assessing security considerations throughout the implementation process. Most importantly, the audit could help identify and address potential problems in system development early in the process.

Public Defender Case Management System

This system used by the Office of the State Public Defender (OPD) for case management, as well as tracking and reporting time spent on cases. Attorneys are required by statute to record their case activity by court and by case type. This tracked information includes the specifics of individual cases worked by state attorneys, correspondence relating to cases, personally identifiable information, financial details (e.g., payments, deposits, vouchers), and detailed schedules. The system spans the 11 regions of the state established by OPD and serves roughly 300 users, including attorneys and their staff, appellate defenders, and administrators. Annual cost and maintenance of the system runs $120,000, including vendor costs and hosting services at SITSD's data center. OPD is currently exploring the feasibility of expanding access to the system to include external parties such as contractors and clients. While assisting with other audits, we identified risks with the access to and security of sensitive information, attorney dissatisfaction with system efficiency, and the potential integration of external parties with a system that is already managed independently by each office. Potential audit topics include (1) Examining factors that would affect data integrity including management of data from multiple decentralized locations, (2) Evaluating system usability to reduce burden of time reporting by public defenders and evaluate system modules to potentially reduce maintenance costs, and (3) Evaluating security of the system ensuring personally identifiable information and personal financial information are protected.

Information Systems Audit Prioritization Calendar Year 2020

eGovernment Services in Montana

The State Information Technology Services Division (SITSD) currently contracts with a vendor for state and local eGovernment services such as payment portals, secure file transfer, and system development. The contract was set to expire in 2019, however based on provisions within the contract a one-year extension has been granted. In August 2018, SITSD signed a letter outlining the decision to further negotiate with the vendor, therefore extending the contract to December 2020. SITSD is currently in the process of developing a solicitation for future eGovernment services. Although SITSD has oversight responsibility of eGovernment services and the statewide contract, management of agency specific services is decentralized. For example, the current vendor uses a self-funded model which uses transaction fees from payment collections to fund enterprise wide services. A self-funded model allows smaller agencies that do not procure transaction fees to be funded through larger agencies, such as Department of Revenue, who procure large amounts of transaction fees. However, because of this model there is risk that the smaller agencies may not receive equal priority for services because they do not process larger transaction fees without centralized oversight. Additionally, because of the decentralization and the nature of services, there is not an easy way to determine the total payments made to the vendor or the cost of contracted services to date. An audit could provide a review of the management over eGovernment services as well as ensuring clear oversight is defined in the contract. Additionally, due to highly confidential information the vendor manages and the high dollar value it brings to the state, an audit could include security assessments over said services.

State of Montana Benefit Plan Eligibility and Administration System

The Health Care & Benefits Division (HCBD) within the Department of Administration implemented a new state employee benefits administration and enrollment system this year. This cloud-based solution was a sole source procurement that replaces and enhances functionality provided by the Statewide Accounting, Budgeting and Human Resources System (SABHRS). Vendor payments are calculated per employee per month, so the estimated ongoing cost of this solution is $700,000 per year. Because this is a cloud solution, sharing information with in-house systems can be a challenge. Information is now manually passed back-and-forth between the two systems for benefit deduction reconciliation. To start the employee benefit enrollment process, the State Human Resources Division provides employee and retiree information to the benefit administration system to determine eligibility. After employees make benefit selections, this system creates a file to manually interface with SABHRS so proper benefit deductions can be made on each employee's paycheck. A file of actual deductions is then created from SABHRS and sent back to the benefit administration system for reconciliation. Manual processes like this can be inefficient and require specific security controls, which is important because this system contains confidential employee information. Security was initially assessed prior to implementing the system by the State Information Technology Services Division (SITSD). While security measures may be clearly documented in agreements with cloud solutions, user controls and monitoring of security is still a shared responsibility. In this case, that would include HCBD, SITSD, and the vendor. An audit could review the efficiency and security of manual business procedures, security governance between multiple entities, risk assessment procedures, and cloud security monitoring to ensure state employee information is protected.

Information Systems Audit Prioritization Calendar Year 2020

Risk Area Definitions:

Regulatory Requirements: represents the amount of legal or contractual requirements of the system or data within the system as well as the level of complexity and volatility of those requirements and the impact on the ability to comply.

Rating Description: Higher classifications indicate few documented requirements of the system or complexity and volatility of current requirements pose risk in the organization's ability to comply.

Topic of Interest: represents any interest from the Legislature, the public, or other audit work.

Rating Description: Higher classifications indicate higher levels of interest and prior audit issues.

Security Management: represents the level of risk associated with the security management and risk assessment procedures of an organization, as it relates to the specific system.

Rating Description: Higher classifications indicate minimal security management policies, monitoring, or assessments with a higher impact if a security incident were to occur.

Impact of System Failure/Issue: indicates the level of risk associated with errors in the system due to flawed, manipulated, or missing data; change control processes; and continuity of operations if affected by a disaster or system failure.

Rating Description: Higher classifications indicate the data within the system is critical or failure within the system poses a high risk.

Management and Governance: defined by the structure, oversight, and management procedures the department has related to the topic/system.

Rating Description: Higher classifications indicate minimal governance or ability to manage the system.

Potential for Fraud/Abuse: shows the potential for fraudulent activity to occur based on review of fraud controls, likelihood of fraud or abuse due to the nature of the data or operations associated with the system, and historic information about the system or program.

Rating Description: Higher classifications indicate known weaknesses or high likelihood of fraudulent activity or abuse due to sensitive data or processing associated with the system.

Nature and Profile: defined by the complexity, age, and cost of a system; number of users; levels of security within a system; criticality of system operations; sensitivity of information processed; and reliance on decisions a system executes.

Rating Description: Higher classifications indicate an expensive, aged, complex system(s) with multiple users and levels of security, and critical operation support with a significant reliance on system output.

2020 Information Systems Audit Topics

Score 1-4
1 = Low Priority
2 = Medium Priority
3 = High Priority
4 = Very High Priority

(no score assigned will result in the assumption of low priority; meaning a score of 1 will be applied)

General Information		**Risk Areas** **Shaded Red = High Risk** **Shaded Yellow = Medium Risk** **Shaded Green = Low Risk**						
Agency	**System/Technology**	**Regulatory Requirements**	**Topic of Interest**	**Security Management**	**Impact of System Failure/Issue**	**Management and Governance**	**Potential for Fraud/Abuse**	**Nature and Profile**
FWP	Licensing & Reservation System (Explore MT)							
OPD	Public Defender Case Management System							
DOA	eGovernment Services in Montana							
DOA	State of Montana Benefit Plan Eligibility and Administration System							

Additional Audit Topics You Would Like Us To Consider for 2021 Calendar Year: