LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller
Miki Cestnik

System Security & Reliability Audits

<u>Audit Objectives</u> ***(what the audit intends to accomplish or questions auditors will answer)*:**
The objective of security and reliability audits is to determine if systems are operating in a controlled environment to increase security and reliability of the system. State law establishes the expectations of departments for ensuring an adequate level of security, therefore these audits seek to identify if agencies are complying with specific requirements to:

- develop and maintain written internal policies and procedures to ensure security of data.
- designate an information security manager to administer the department's security program for data;
- implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data;
- ensure that internal evaluations of the security program for data are conducted.
- include appropriate security requirements, as determined by the department, in the written specifications for the department's solicitation of data and information technology resources

Appropriate safeguards include those required by state policy, and those required by external entities, such as the federal government. These audits focus on those safeguards and provide a report on agency compliance.

<u>Audit Scope</u> ***(The boundary of the audit and subject matter that auditors will assess)*:**
Security and reliability audits focus on critical systems within state government. these systems can be complex, comprised of multiple application or services. Therefore, a risk assessment is done to identify the areas of the system that need stronger controls and have larger impacts to the agency, public, or state government. Scoping also considers what safeguards to assess. Not all safeguards, policies, and procedures can be reviewed in a single audit, therefore areas of review are determined based on the risk we identify related to system security and reliability.

GenTax (24DP-05) - Department of Revenue

- System components within scope: GenTax system, which encompasses system processes to manage state taxes, gambling tax, livestock per capita fee program, marijuana dispensary licensing, and Agriculture's commodities reporting and payments.
- Safeguards: Access Management, Awareness and Training, Configuration Management, Contingency Planning, Identification and Authentication, and System and Information Integrity

Medicaid Enterprise System (24DP-03) - Department of Public Health and Human Services

- System components within scope: Pharmacy Claims Processing and Management Services (MMIS) and Pharmacy Support Services (FlexRx)
- Safeguards: Access Management, Awareness and Training, Security Assessment and Authorization, Security Planning, Risk assessment, System and Services Acquisition, Configuration Management, Contingency Planning, Identification and Authentication, and System and Information Integrity.

Most agencies operate in a shared control environment, where either the State Information Technology Services Division (SITSD) or a vendor own some of the controls in the areas of review. Controls owned by SITSD and vendors are not included in these audits. However, if there are significant controls owned by a vendor, the process for how the agency evaluates or assures vendor controls is reviewed.

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