GENTAX

DEPARTMENT OF REVENUE

FEBRUARY 2025

24DP-05

System Security and Reliability Audit

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.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver, Legislative Auditor

Audit Staff

Miki Cestnik, CISA, CRISC
Gonzalo Lazalde
Deborah Stratman

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

MONTANA LEGISLATIVE AUDIT DIVISION

SYSTEM SECURITY AND RELIABILITY AUDIT

A report to the Montana Legislature

Angus Maciver, Legislative Auditor

Background

GenTax is the state tax administration system operated by the Department of Revenue, managing just over $4 billion and handling federal tax information (FTI), criminal justice information (CJI), and personally identifiable information (PII). The system has many external stakeholders, which impacts agencies, businesses, and individuals in Montana. It provides tax information to the Governor's Budget Office and to the Legislature for budgeting and economic forecasting, as well as supplying alcohol inventory information for state liquor sales. The agency is highly dependent on GenTax, with 80 percent or more of its internal resources requiring it for its operations.

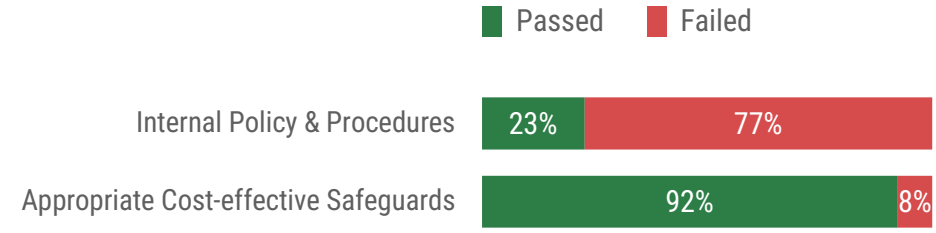
GenTax is a highly customizable, commercial off-the-shelf (COTS) system provided by a vendor, configured to fit the DOR's needs. The State Information Technology Services Division (SITSD) provides infrastructure support for GenTax, and the vendor performs system maintenance.

GenTax

The Department of Revenue (DOR, agency) is managing the control environment for GenTax; however, we identified areas for improvement. These areas include formalizing and adopting internal IT control policy and procedures and improving safeguards related to the agency's contingency planning capabilities. The figure below summarizes testing across two key areas that help form the foundation of the control environment, encompassing the standards, structures, and processes essential for effective internal control.

Figure 1

The Department of Revenue needs to formalize and adopt internal IT control policy and procedures and improve elements of its cost-effective safeguards.



Source: Compiled by the Legislative Audit Division.

What We Did

The objective of security and reliability audits is to evaluate whether systems are operating within a controlled environment that enhances their security and reliability. Our assessment was based on the data security responsibilities outlined in §2-15-114, MCA, and IT security policy established by SITSD within the Department of Administration (DOA). Due to handling Federal Tax Information (FTI), GenTax must also comply with Internal Revenue Service (IRS) Publication 1075. This publication and State IT policy are based on the same industry standard; however, our audit identified some minor differences. We used the most strict standard of the two for our audit.

Due to the extensive number of standards for GenTax, we did not review all security standards. Because of GenTax's importance and impact on state income taxes, use of individual income information across state government for other programs' administration, and reliance on accurate information by the legislature, the controls identified within scope relate mostly to the reliability of the data within GenTax. Other control areas may be assessed in future audits through our risk-based approach. The specific control areas within the scope of our audit are further defined in Table 1.

Table 1
Control Areas Within Scope

Control Areas	Abbreviation	Description
Access Control	AC	Determines when and how users can access the system and their level of access.
Identification & Authentication	IA	Recognition and verification of allowed system users.
Configuration Management	CM	Baseline structure, inventories, and a security impact analysis control.
System & Information Integrity	SI	Flaw remediation, malicious code detection, information systems monitoring, security alerts, software, firmware integrity, and spam protection.
Contingency Planning	CP	Contingency plan testing, updating, training, backups, and system reconstitution.
Awareness & Training	AT	Security training, procedures, and training records.

Source: Compiled by the Legislative Audit Division.

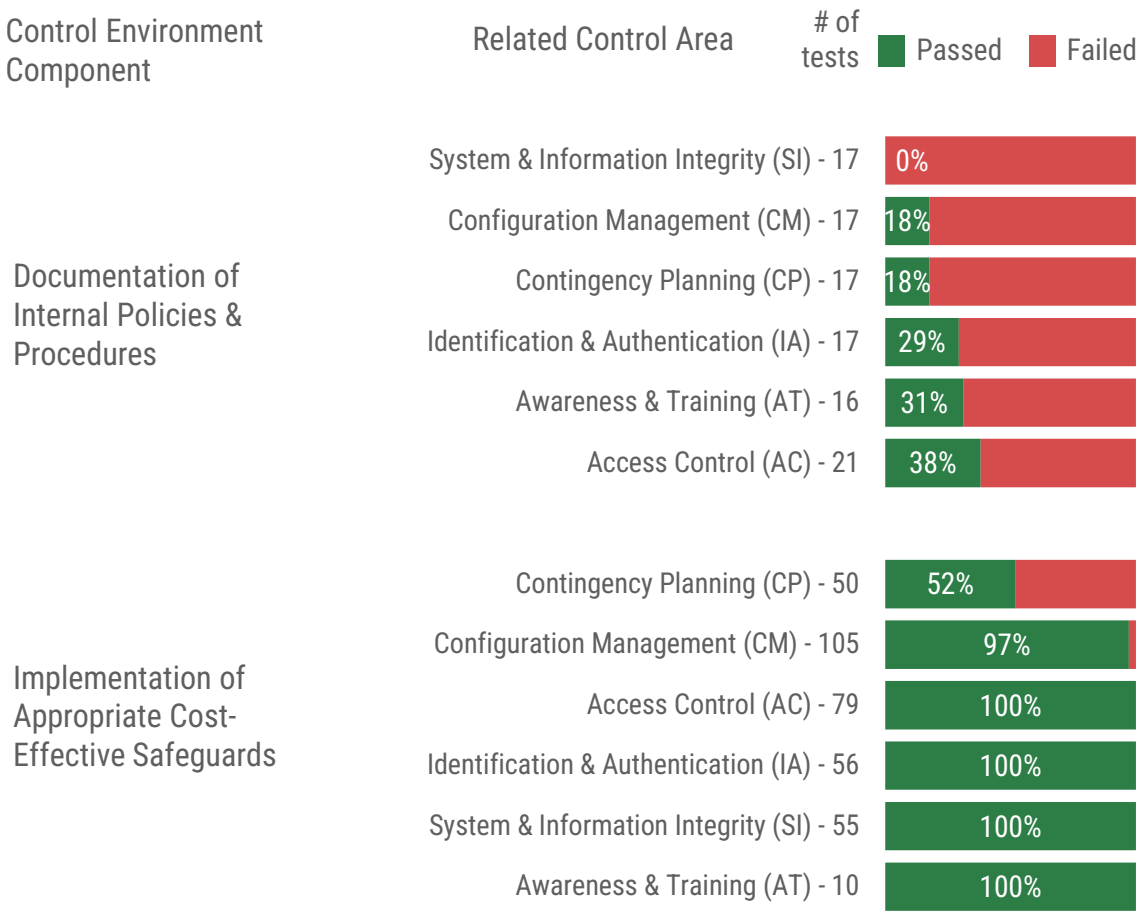
Our testing methods involved interviewing agency personnel and reviewing external audits, system security plans, and any available agency documentation. For this audit, we reduced the number of tests we conducted by relying on the work performed by the Internal Revenue Service (IRS) Safeguard Review Team (SRT). Our audit scope included 426 controls. By relying on the work of the SRT, we reduced the number of controls we tested to 115. We reperformed SRT testing for controls in the Access Control (AC) family and identified no issues as required by auditing standards.

What We Found

Five of the six safeguard areas we tested had few or no issues, while the Contingency Planning safeguard and the agency's internal policies and procedures present opportunities for improvement. Figure 2 (page 3) provides a summary of our audit testing across each area of the control environment.

Figure 2

Report Card:
Test results highlight notable progress and opportunity.



Source: Compiled by the Legislative Audit Division.

The Department of Revenue Relies on the Limited Policy and Procedures Established in State Policy by SITSD

The agency has limited policies and procedures related to the control areas tested; instead, it relies on SITSD's Information Security Policy (ISP) and other standards. It had only one documented policy specific to Configuration Management (CM). However, that policy's applicability was limited to only one out of 11 controls in the CM area.

The language in the ISP provides some guidance and understanding, but it is incomplete. The ISP indicates that agencies can develop policy and procedures for individual systems. The agency should address the decisions and procedures specific to its systems through its policy and procedure documentation.

The Department of Revenue's Contingency Planning Requires Better Documentation and Improved Management

In the event of an unforeseen emergency, contingency planning helps in managing the crisis when it arises and reduces the likelihood of damage to an agency's operations. We identified failures in critical areas of documenting a plan, testing it, and training staff on executing it. We also identified failures in awareness of details pertinent to the operations performed at a backup location when the primary site is unavailable due to an emergency (alternate site processing). Specifically, the agency does not:

- Have a contingency plan with required administrative details.
- Perform training on the contingency plan as required.
- Test the contingency plan as required.

Due to turnover in critical roles related to contingency planning (CP), the DOR lost the institutional knowledge necessary to adequately understand and follow SITSD's management of the operations at the alternate site.

Impact

Policies and procedures are essential to ensure organizational systems continue to function effectively, regardless of staff changes. They provide clear, consistent instructions for operations, reducing reliance on institutional knowledge and mitigating the risk of losing critical expertise due to staff turnover. This issue became evident during our fieldwork when the Information Protection Office (IPO) staff departed from the agency. The absence of robust policies and procedures resulted in challenges for the remaining staff in understanding and implementing contingency planning effectively. Without the IPO's leadership, the DOR's ability to manage unanticipated events is potentially compromised due to the lack of a comprehensive contingency plan and inadequate training and testing to support its execution.

Furthermore, policies should clearly specify which standards to follow when systems are subject to multiple compliance requirements. For instance, GenTax must adhere to both State policy (MT-BASE) and IRS Publication 1075 standards. Without clear guidance, organizations risk complying with one standard while falling short on another. During our review, we observed this issue in configuration management. While DOR adhered to IRS Publication 1075, it failed to meet the stricter state policy requirements in three of the 11 tests conducted in this area.

Improvement Opportunity

The Information Protection Office within the DOR has historically played a pivotal role in policy development, management, and the coordination of contingency planning. Long-tenured staff effectively ensured compliance with IRS standards and maintained the agency's security program. However, the reliance on a single office staffed by only two full-time employees (positions budgeted, PBs) created a significant risk when both positions in the office became vacant. During the audit, the DOR faced challenges filling these critical positions, highlighting the growing demand and competitiveness in security management and cybersecurity.

The agency has reassessed the office's responsibilities with recently onboarding new IPO staff. The agency has indicated that more governance and policy decision-making authority will now be assigned to the Chief Information Officer, while the IPO will focus on maintaining policies and procedures and managing compliance. This shift in responsibilities could strengthen the DOR's overall security program. However, there are still specific areas where the agency can improve further to enhance its effectiveness.

The Department of Revenue Needs To Identify and Develop Agency and System Specific Documentation

The agency relies on high-level enterprise policy and has only a few procedure documents for most areas we reviewed. As a result of this reliance, the lack of procedures, and more actively managing compliance with IRS Publication 1075, the DOR is not meeting state security requirements for GenTax in a small number of our tests. As security standards evolve and state policy continues to improve, this may not always be the case. It would benefit the agency to develop a compliance matrix to verify which standards are the most appropriate and then incorporate the most appropriate controls into its policy and procedures. Actively managing such a matrix while standards change will ensure the agency is always aware of differences and can intentionally choose which standard to follow or if they need to follow the most stringent requirements from each.

Recommendation #1

We recommend the Department of Revenue:

A. Review IRS Publication 1075 and state policy to identify differences in standards and document, through policy, the decisions about which standard to implement,

B. Work with SITSD to identify areas where system specific policy needs development,

C. Develop and implement system specific procedures, and

D. Formally adopt and supplement state IT control policy and procedures.

The Department of Revenue Has Implemented Most of the Cost-Effective Safeguards We Tested

The Department of Revenue successfully met 328 out of 355 safeguard test requirements, achieving an overall pass rate of 92 percent. The Access Control, Identification and Authentication, System and Information Integrity, and Awareness and Training control areas fully met all criteria, while Configuration Management had only three deficiencies. These deficiencies were not due to missing safeguards but resulted from configurations designed to comply with IRS Publication 1075, which differs from state policy requirements. We identified an opportunity for improvement in the Contingency Planning control area, where we found 24 deficiencies.

The Department of Revenue Needs To Improve Its Contingency Planning Capabilities

Continuity and Contingency Planning policy at the state level continues to develop, contributing to the lack of such planning at the agency level. Currently, Montana Disaster and Emergency Services (DES), situated within the Montana Department of Military Affairs (DMA), spearheads continuity as part of its role as the lead agency coordinating comprehensive emergency management in Montana. While DES has a lead role in coordinating and guiding agencies in preparedness and continuity, it does not include technological aspects such as cybersecurity threats. Instead, it provides standard guidance from federal agencies. SITSD coordinates federal Department of Homeland Security (DHS) cybersecurity tabletop exercises for the state agencies. Consequently, DES and SITSD each play a part in establishing and guiding continuity and contingency activities for agencies, with DES handling the business and administrative planning and SITSD handling cybersecurity.

Similar to the state level, the DOR's overall contingency planning is handled by the Continuity Coordinators, who are part of the Director's Office staff and whose experience and expertise are focused on business and operations continuity rather than IT-specific risks within the agency. Without input from the Technology Services Division (TSD) within the DOR, specific details related to safeguards for GenTax may not be included. Without the overall guidance of a robust policy and effective procedures for contingency planning, non-IPO staff, and newly onboarded IPO staff will struggle to effectively understand and manage the controls for which they're responsible.

With the separation of business and technological concerns in guidance at the state level and operations at the agency level, a comprehensive contingency plan is critical to ensure adequate controls are in place. By providing training to all involved staff and testing the plan, the DOR will ensure that everyone involved in an unanticipated event will know what to do when disaster strikes.

Recommendation #2

We recommend the Department of Revenue:

A. Document appropriate information to develop a sufficient continuity plan, and

B. Coordinate contingency activities, training, and testing with both business and technical staff.

DEPARTMENT RESPONSE
DEPARTMENT OF REVENUE

MONTANA
DEPARTMENT OF
REVENUE

GOVERNOR GREG GIANFORTE
DIRECTOR BRENDAN BEATTY

February 19, 2025

Angus Maciver, Legislative Auditor
Performance and Information Systems Audits
Legislative Audit Division
Room 160, State Capitol Building
PO Box 201705
Helena, MT 59620-1705

RECEIVED
February 19, 2025
LEGISLATIVE AUDIT DIV.

Dear Mr. Maciver:

The Department of Revenue herein responds to the Security and Reliability Audit of GenTax.

Recommendation #1A

We recommend the Department of Revenue Review IRS Publication1075 and state policy to identify differences in standards and document, through policy, the decisions about which standard to implement.

Concur. The department will review IRS Publication 1075 and state policy to identify differences, select the standards to follow, and develop and implement policies and procedures that meet the required standards. We are waiting for the State Information Technology Services Division (SITSD) to release the latest update to the state's policy for information security. Once the updates are released, we will compare the updated state policy to the IRS standards and review department policies and procedures and update accordingly.

Recommendation #1B

We recommend the Department of Revenue work with SITSD to identify areas where system specific policy needs development.

Concur. The department is willing to work with the SITSD to identify areas where specific policies and procedures are required and which standards should apply.

Recommendation #1C

We recommend the Department of Revenue develop and implement system specific procedures.

Concur. The department will develop and implement system-specific procedures as the selected standards require.

Recommendation #1D

We recommend the Department of Revenue formally adopt and supplement state IT control policy and procedures.

Concur. The department will formally adopt and supplement state IT control policies and procedures as appropriate. We will work with SITSD to determine which state IT policies and procedures should be adopted.

Recommendation #2A

We recommend the Department of Revenue document appropriate information to develop a sufficient continuity plan.

Concur. The department will document a continuity plan that encompasses GenTax operations from a technical and business perspective. The plan will not address continuity of non-GenTax systems or business operations.

Recommendation #2B

We recommend the Department of Revenue coordinate contingency activities, training, and testing with business and technical staff.

Concur. The department will develop internal procedures and plans to support contingency and continuity for the GenTax system only. The business and technical staff will be trained on their roles and involved in regular testing of the GenTax continuity plans through regular desk-top exercises. The department will monitor and document SITSD testing of alternate site operation and maintenance.

The department believes the portions of these recommendations within our control can be accomplished within 1 1/2 years.

Sincerely,

Brendan Beatty, Director
Montana Department of Revenue