LOTTERY OPERATING SYSTEM (LOTOS)

MONTANA STATE LOTTERY

AUGUST 2026

26DP-01

System Security and Reliability Audit

Legislative Audit Committee

Representatives

Mary Caferro
Mary.Caferro@legmt.gov
Scott Demarois
Scott.Demarois@legmt.gov
Sherry Essmann
Sherry.Essman@legmt.gov
Jane Gillette
Jane.Gillette@legmt.gov
Jerry Schillinger, Chair
Jerry.Schillinger@legmt.gov
Jane Weber
Jane.Weber@legmt.gov

Senators

Becky Beard
Becky.Beard@legmt.gov
Denise Hayman
Denise.Hayman@legmt.gov
Emma Kerr-Carpenter
Emma.KC@legmt.gov
Forrest Mandeville
Forrest.Mandeville@legmt.gov
Tom McGillvray
Tom.McGillvray@legmt.gov
Laura Smith, Vice Chair
Laura.Smith@legmt.gov

Members serve until a member's legislative term of office ends or until a successor is appointed, whichever occurs first.

§5-13-202(2), MCA

Fraud Hotline
(Statewide)
1-800-222-4446
(in Helena)
444-4446
LADHotline@legmt.gov
www.montanafraud.gov

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
Emily Nichols
Deborah Stratman

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

Montana Legislative Audit Division

System Security and Reliability Audit

A report to the Montana Legislature

Angus Maciver, Legislative Auditor

Background

Established by Montana voters in 1986, the Montana State Lottery sold its first ticket in 1987 and has since funded the STEM scholarship program and contributed to the state's general fund. It offers instant win (scratch) games, lotto games, and sports wagering. The lineup includes multi-state options such as Powerball, Mega Millions, Millionaire for Life, and Lotto America, along with state-specific games such as Montana Cash, Big Sky Bonus, and Montana Millionaire. Additionally, the Lottery offers Treasure Play games, another type of instant win lotto. Over time, the Lottery has awarded more than $1 billion in prizes, contributed over $350 million to the State of Montana, and generated more than $100 million in commissions for sales agents.

Lottery Operating System (LOTOS)

The Montana State Lottery (Lottery, agency) oversees the control environment for the LOTOS, the Lottery operating platform. Although the vendor owns LOTOS' core technology and its control environment, the agency is responsible for its governance and procedural oversight. The new contract, commencing in 2026, presents a vital opportunity for the Lottery to implement strong governance and procedural oversight, addressing past shortcomings. These included struggles with risk management, inadequate identification of vendor security requirements, and improper allocation of IT security roles, whose incomplete resolution made vendor oversight the highest-risk area. The figure below summarizes our testing of the agency's implementation of controls for system and service acquisition, a key area we identified as the greatest risk to the agency. This testing encompasses the standards, structures, and processes essential for effective internal control.

Figure 1

Procurement and contract documentation establish the foundation for success, but the agency must ensure vendor compliance.

Control Environment Component	Related Control Area	# of tests	Passed	Failed
Security Requirements within Written Solicitations	System and Services Acquisition (SA)	79	72%	28%

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. We based our assessment on data security responsibilities outlined in §2-15-114, MCA.

We also considered the requirements of §23-7-411, MCA, for auditing state lottery security, and the IT security policy established by the State Information Technology Services Division (SITSD) with the Department of Administration (DOA). State IT policy is based on industry standards; however, there are some minor differences.

Because the LOTOS must adhere to many security standards, we could not review all of them. Our risk-based approach identified the agency's oversight of vendor security compliance as a high risk. Given the LOTOS's critical importance to the Lottery and the agency's reliance on its vendor, vendor control assurance practices represent the highest risk control area: System and Services Acquisition (SA).

The SA control area addresses security throughout the system development lifecycle, third-party acquisitions, and IT security contract management. For example, controls cover developer testing, security engineering principles, and outsourced information system services. While we reviewed the procurement and contract documentation, we did not review the procurement process itself, as another team was performing that review. Future audits may assess other control areas using this risk-based approach.

Our testing methods involved interviewing agency personnel, reviewing security plans, and evaluating supporting evidence for duties and responsibilities. For this audit, we also included a thorough examination of procurement and contracting documentation.

Prior Audit Work

The Lottery Security (23DP-02) report was issued to the Legislative Audit Committee in October 2023. The audit included two recommendations to the Lottery that focused on risk assessment and risk management. As part of this security audit (26DP-01), we conducted follow-up work to assess the implementation of the report recommendations.

Recommendation #1

We recommend the Montana State Lottery seek the education or training necessary to implement effective risk management and establish an appropriate role for audit within risk management.

Implementation Status: Being Implemented

The Montana State Lottery has hired a qualified Information Systems Security Officer (ISSO), improved the role of audit, and developed a draft information security policy, showing progress toward full implementation.

Recommendation #2

We recommend Lottery establish a risk management program that aligns with state policy that includes:

A. Appropriate risk assessment methods for the collection of risk-related data, analysis of this data for risk identification, and maintenance of a risk profile, and

B. An inventory of applicable state policy requirements and a method to track and ensure satisfaction of these requirements

Implementation Status: Being Implemented

The Lottery has made progress in risk management, implementing procedures and adopting the state's security management system.

A. While risk identification and monitoring activities have begun, a formally approved risk assessment methodology and governance workflows for maintaining a risk profile are incomplete or unapproved.

B. Foundational elements are in place, but documentation for an inventory of applicable state policy requirements and a method to track and ensure their satisfaction remains incomplete or unapproved.

What We Found

Despite well-written procurement and contracting documentation, the Lottery has not established clear processes or assigned specific responsibilities for managing vendor compliance and IT security within its contracts.

The Lottery's mission relies on its operating platform, which demands continuous readiness and robust security. The contract clearly outlines operational and security expectations, combining requirements from the Request for Proposal (RFP), vendor commitments, and state IT terms. To ensure the vendor meets these expectations, the Lottery needs processes and staff to monitor and manage the contract. Ensuring vendor compliance with standards from the Multistate Lottery Association (MUSL) and SITSD is crucial to safeguarding the Lottery's platform and data.

The Lottery recently entered into a new contract with its external service provider following a competitive procurement process, continuing a relationship that spans nearly two decades. A key control we reviewed requires the agency to define, monitor, and manage security requirements to external service providers.

We identified various ways these requirements are described.

- The new contract includes performance standards to which the vendor has committed.
- The vendor has agreed to comply with the requirements in the agency's RFP.

- The agency provided evidence for the vendor's system development life cycle, security engineering principles, developer configuration management, security testing and evaluation, development processes, standards, and tools.
- The vendor committed to ensuring continuous support for the platform's system components.

While procurement and contracting documentation described security requirements, the agency did not supply documentation indicating how it would monitor and manage them. We identified missing documentation as an area of improvement, especially as the Lottery continues to manage this contract through March 2033.

Montana State Lottery Faces Challenges in Vendor Compliance and Security

Personnel changes, such as the hiring of a new Information Systems Security Officer and the retirement of the Director of Security, have impacted the Lottery's capacity to ensure vendors follow contract security rules. The agency has not created policies or procedures to ensure vendor security compliance. Additionally, it has not clearly assigned contract management duties or outlined how security responsibilities are divided between the vendor and the Lottery.

This lack of clarity complicates the implementation of the agency's high-level information security requirements. Without a clear framework that defines who is responsible for what tasks, who must approve decisions, and who needs to be informed, gaps in security work can go undetected. Similarly, the agency has not clearly assigned specific duties to monitor and manage vendor compliance with contracts. This means the agency does not adequately define, monitor, or manage security requirements for outside service providers, leaving it without a documented way to oversee or enforce vendor compliance.

At the time of our review, the agency also had not yet obtained or developed essential system, component, and service documentation, such as administrator guides, user guides, or system design documentation. However, this information is part of security requirements in the contract and is expected to be provided to the Lottery within ten business days after implementation of the new system. Implementation was originally scheduled for July 26, 2026, but was moved to August 30, 2026. Therefore, we do not consider this to be a deficiency if the vendor fulfills its contractual obligation.

To reduce risk, the agency must strengthen its operational processes, particularly in documentation, staffing, and vendor oversight, to ensure that security requirements are not only contractually defined but also consistently implemented and verified.

Impact

These findings significantly impact how the Lottery manages and assures security and contract performance. Inadequate definition, monitoring, and enforcement of security requirements for external service providers create significant vulnerabilities for the agency, including increased risks of data breaches, system compromises, and operational disruptions. This could also challenge effective incident response, potentially resulting in regulatory noncompliance and notable financial and reputational impacts.

Without a clear responsibility matrix and defined roles for contract compliance, the Lottery can face significant operational and security challenges. This incomplete implementation creates confusion in roles and responsibilities, leading to inefficient resource allocation and accountability gaps, which in turn increase the agency's overall risk exposure. Furthermore, under-resourcing for information security often limits strategic planning and forces a reactive approach, reducing the agency's ability to meet its security requirements effectively.

Lottery Has Made Improvements from the Previous Contract

The Lottery's previous contract with the vendor, effective from March 31, 2016, to March 30, 2026, did not clearly define system security requirements. Although the contract allowed for liquidated damages if the vendor failed to meet security requirements, it did not define a security incident. This required the agency to interpret security incidents based on statute. Without explicit contractual language, the agency's ability to enforce vendor security practices through liquidated damages was limited.

Liquidated damages are an important enforcement mechanism, particularly because lottery and sports wager data lack the robust legal protections of Federal Tax Information (FTI) or Criminal Justice Information Services (CJIS) data. Disclosing FTI or CJIS data without authorization carries criminal, civil, and professional consequences, thus incentivizing vendors who handle such sensitive information to maintain secure and reliable systems.

This limited enforcement became evident in late 2025, when the current ISSO conducted the agency's first compliance assessment of the previous contract. This assessment revealed four instances of vendor noncompliance with IT security practices, one of which persisted unresolved from May 2020 to December 2025. The ISSO calculated nearly $1.7 million in potential liquidated damages for this incident; however, the agency did not pursue these damages because the recoupment period had expired. Had defined monitoring procedures and clear responsibilities been in place, the Lottery might not have missed this opportunity to enforce vendor compliance.

Addressing these past limitations, the new contract now incorporates explicit performance standards for system conversion and ongoing maintenance, making agency monitoring crucial. For instance, the Lottery's system conversion includes three key performance standards, with failure resulting in accrued liquidated damages.

As an example, a five-day delay in contractor testing and a four-day delay in system functionality could result in liquidated damages of $810,000. While this is an illustrative example, it demonstrates the importance of the vendor meeting operational milestones for the Lottery's operations platform.

Improvement Opportunity

In the past, the Lottery has struggled to effectively identify and monitor compliance with security requirements in these large, complex contracts. The Lottery Security Audit (20DP-01), presented to the Legislative Audit Committee in October 2021, highlighted similar issues. Our follow-up work noted progress in some areas of these recommendations. In contrast, others, like formalizing IT security policies and procedures, developing IT risk assessment processes, and defining security requirements have yet to be implemented. These mission-critical contracts provide services to each division within the agency. They require adherence to performance and security standards and necessitate clear monitoring controls.

Unclear IT Security Duties and Staffing Issues Impact Lottery's Vendor Oversight

The IT Services Director and Information Systems Security Officer procedure manuals both discuss IT security and vendor management responsibilities. The IT Services Director's manual assigns contract management, but with minimal scope details. Only 22% of 391 security requirements from the RFP are explicitly assigned to either the IT Services Director or the ISSO, creating significant ambiguity in vendor contract management.

Neither document clearly defines IT Security duties. The IT Services Director's manual mentions transferring these duties to the ISSO, but provides no timeline or specifics, while the ISSO's manual merely references IT Security without defining the duties. Documenting duties and responsibilities for contract compliance management is essential, for example, in job or position descriptions, procedure manuals, and policies.

The Lottery's new Contract Compliance Monitor position further complicates vendor oversight. This role, intended to monitor vendor compliance, encompasses 13 diverse duties, including contract compliance, financial analysis, internal controls, and audit support. This broad scope requires a highly skilled and experienced professional, yet the advertised salary range of $50,000 to $58,000 is significantly lower than comparable state positions, which typically start at $69,000 to $72,000. The position opened March 23, 2026 and closed June 21, 2026.

The agency reported difficulty attracting suitable candidates, finding that applicants did not meet the desired qualifications. Consequently, the agency is revising the job description, acknowledging it initially sought an internal auditor, which is a role distinct from contract compliance, and it is considering an increased pay range. This recruitment challenge suggests the agency has not yet clearly defined its needs or translated them into an appropriate position. Given the vague nature of the position's contract compliance aspects, it remains unclear who currently manages these duties. The contract assigns ultimate responsibility for managing the vendor contract to the IT Services Director, a responsibility confirmed in their Desk Manual. However, this manual provides minimal detail on the specific tasks involved.

A Needs and Risk Assessment Would Clarify Lottery's Security and Contract Management

Both a focused needs assessment, including staffing requirements, and a risk assessment should have been conducted during contract development. Previous audit recommendations identified the need to define security requirements and perform risk assessments; however, the agency delayed implementing risk management until a new ISSO was hired. This delay slowed the development of risk management within the Lottery and resulted in security requirements remaining unidentified and unmonitored in the new contract. However, the ISSO is now performing the assessment and the review of security requirements.

A needs assessment would identify both compliance requirements and risk-based needs. This systematic process evaluates gaps between a current situation and a desired outcome, helping an organization identify problems, prioritize actions, and develop targeted solutions. For the Lottery, such an assessment is crucial because state policy compliance requirements vary significantly by system type. For instance, one set of requirements applies to systems that handle federally regulated information. At the same time, another establishes a baseline of critical controls for vendor-managed systems that do not process such information.

The State Information Technology Services Division directs the Lottery to use the baseline of critical controls for vendor-managed systems rather than the more extensive version. However, the baseline controls omit a key control for effective contract management. This missing control would document roles and responsibilities, define and enforce compliance, and monitor ongoing adherence to the agency's security standards for external services. This omission hinders comprehensive contract management policies and can create a reactive approach to contractor requirements. Despite this, the agency remains responsible for implementing appropriate safeguards, including best practices, that incorporate the control.

This responsibility is critical given that, due to multiple competing priorities, the ISSO has only recently started documenting RFP requirements, exposing a historical gap in these vital processes.

Recommendation #1

We recommend the Montana State Lottery:

A. Perform a Contract Compliance needs assessment to clearly define vendor commitments, duties and responsibilities for monitoring, managing, and enforcing vendor contracts,

B. Assign the identified duties and responsibilities to specific roles within the agency,

C. Develop a framework that identifies the shared responsibility between the vendor and the agency, and

D. Document Contract Compliance duties and responsibilities and implement methods to continuously monitor external service provider compliance with contractual obligations.

LOTTERY RESPONSE

MONTANA STATE LOTTERY

MONTANA LOTTERY

August 04, 2026

Mr. Angus Maciver
Legislative Auditor
Office of the Legislative Auditor
State Capital Building
Helena, MT 59620-1705

RECEIVED
August 4, 2026
LEGISLATIVE AUDIT DIV.

RE: Response to the 2026 Montana Lottery Security and Reliability Audit

Dear Mr. Maciver:

The Montana Lottery has received the results of the 2026 Legislative Security and Reliability Audit and appreciates the opportunity to provide input on the recommendations. The agency values the Legislative Audit Division's recommendations and views these findings as an opportunity to strengthen our security posture and compliance with state and federal requirements.

We at the Montana Lottery concur with the single four-part recommendation. Under the authority of the new vendor contract, agency staff have identified the changes needed to implement the recommendations and will ensure they are implemented as the system conversion is completed, including updates to oversight processes and desk manuals.

We recommend the Montana State Lottery:

A. Perform a Contract Compliance needs assessment to clearly define vendor commitments, duties, and responsibilities for monitoring, managing, and enforcing vendor contracts:

The Montana Lottery plans to develop and implement a formal contract compliance assessment process for the agency's various contracts. This process will define assessment frequency, scope, and criteria, including conformance with contract terms, applicable state and federal requirements, and agency policies. Results will be documented and reported to management.

B. Assign the identified duties and responsibilities to specific roles within the agency:

With the documented contract compliance assessment results, management will clearly assign and ensure proper documentation of the roles responsible for contract compliance activities, including monitoring contractor performance, reviewing deliverables, validating adherence to requirements, and coordinating remediation of any issues identified.

MONTANA LOTTERY

C. Develop a framework that identifies the shared responsibility between the vendor and the agency:

The Montana Lottery plans to enhance and optimize the existing framework provided in the vendor contract to clearly define how the contractor and agency coordinate on contractual obligations, including security-related deliverables, performance metrics, reporting, and issue escalation. This enhanced framework will be documented in companion governance materials, such as service-level agreements, procedures, and oversight guides, and will ensure enforcement of security incident reporting, vulnerability remediation timelines, change management, and compliance attestations. The agency-specific framework will be applied to the current vendor contract and used as a reference for managing similar engagements.

D. Document Contract Compliance duties and responsibilities and implement methods to continuously monitor external service provider compliance with contractual obligations.

Montana Lottery management must ensure relevant desk manuals and procedural documentation will incorporate contract compliance duties for the agency, including step-by-step guidance for conducting assessments, recording results, engaging the contractor on findings, and escalating noncompliance. Documentation will be maintained in a central location and provided to all staff involved in contract oversight as the most relevant standard reference for day-to-day compliance activities. The proper documentation ensures repeatable procedures that create measurable data for management evaluation.

The Montana Lottery is committed to fully implementing these corrective actions and incorporating them into our ongoing operations. By strengthening our security governance, formalizing processes, and enhancing documentation, we will improve oversight, support informed management decision-making, and further protect our information technology environment. We anticipate these changes to be fully implemented before the end of the fiscal year. We appreciate the professionalism and collaborative approach of the Legislative Audit Division throughout this audit and thank the audit team and Legislative Audit Committee for their constructive recommendations and continued commitment to improving state government.

Sincerely,

Bob Brown, Director
Montana Lottery