A Report
to the
Montana
Legislature

Information Systems Audit

Lottery Security

Montana State Lottery
Department of Administration

October 2021

Legislative Audit
Division

20DP-01

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS 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 IS 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 IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS 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.

Audit Staff

Miki Cestnik
Amanda Sayler
Tyler Julian

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

LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller

October 2021

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an information systems audit of Montana State Lottery security operations. Montana law requires the Legislative Audit Division to perform a comprehensive security audit of the Montana Lottery every two years. Starting in calendar year 2020, we assessed security controls within the 18 security areas defined by statute, including Lottery's computer systems, scratch and online tickets, and Lottery personnel and sales agents.

This report contains five recommendations for strengthening contractor security assurances, formalizing system testing procedures, and improving business continuity procedures. A written response from the Montana Lottery is included at the end of the report.

We wish to express our appreciation to the Montana State Lottery personnel for their cooperation and assistance during the audit.

Respectfully submitted,

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Montana State Lottery	Scott Sales, Director (beginning May 2021)		
	Angela Wong, director (through December 2020)		
	Bryan Costigan, Security Director and Acting director (January 2021 through May 2021)		
	Phil Charpentier, Information Technology Director		
Department of Administration	Misty Ann Giles, Director (beginning January 2021)		
	John Lewis, Director (through December 2020)		
			Term Expires
Lottery Commission	John Tarr, Chair	Helena	1/1/2022
	Tony Harbaugh, Law Enforcement	Livingston	1/1/2025
	Thomas M. Keegan, Attorney	Helena	1/1/2022
	Leo Prigge, CPA	Butte	1/1/2023
	Steve Morris, Public Member	Helena	1/1/2025

Information Systems Audit 20DP-01 October 2021

Montana Legislative Audit Division

Lottery Security

Montana State Lottery and the Department of Administration

While Lottery has made progress implementing risk management procedures since the last audit, there are still areas being developed and key areas that need more attention. Our work this cycle identified the need for more transparency and accountability for contractors within the cyber supply chain of Lottery's services, improved testing plans when new functionality or services have legal requirements, and better management of continuity planning.

Background

The Montana State Lottery (Lottery) was created in 1987 and has contributed significant funds to various state programs and the general fund. In fiscal year 2020, Lottery sales from online and scratch ticket games were approximately 59.9 million. While this is a 3.7 million decrease from previous fiscal year sales, likely due to the current pandemic, Lottery was still able to increase sales to over $112 million in fiscal year 2021 with the addition of sports betting.

Online and scratch ticket games are managed by Lottery and the systems and gaming services are provided to Lottery by contractors. Lottery uses one main contractor for providing most gaming services. This contractor's systems support main lottery operations, random number generators, independent verification of lottery operations, and the newly established Sports Bet Montana system. A separate contractor provides scratch tickets to Lottery.

KEY FINDINGS:

Current Security Requirements Are Not Being Met. Multiple documents from the contracting process outline security requirements for Lottery's operating system. However, the contractor has not met requirements in regard to security planning, subcontractors, securing remote access, business continuity, continuity testing, and backup services.

Lottery Needs to Define Security Requirements to Be Able to Enforce Them. Specific security requirements are scattered throughout a document that is over 800 pages and tools for enforcing these requirements are not clearly stated or defined. Vague security requirements and enforcement tools within the contract set the tone for passive contract management practices.

Current Security Assurances Do Not Cover Critical Cybersecurity Risks. While Lottery receives assurance of integrity over some contractor operations, like scratch tickets and financial transactions, the assurances do not address cybersecurity risks to all of Lottery operations. The report from the gaming system contractor covers a few aspects of IT, but it is only those that would impact transactions and financial statements. It does not include critical areas such as risk management and mitigation procedures, change management, system configuration, vulnerability, or patching.

It Is Not Clear How the New Service Meets Legal Requirements. Various systems are used by the contractor to manage the new sports betting service. As a contractor-managed system, Lottery's needs to verify legal requirements are met by thoroughly testing the system. While test cases addressing some of the more basic functions were identified, there were other system requirements with no related test cases and other activities where the website terms and conditions were not in agreement with administrative rule.

Business Continuity Plans (BCPs) Are Missing Essential Details. The core function of a BCP is to define a business strategy that enables an organization to continue operations during a disruption. Lottery's BCP

(continued on back)

For the full report or more information, contact the Legislative Audit Division.

leg.mt.gov/lad

Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705
(406) 444-3122

The mission of the Legislative Audit Division is to increase public trust in state government by reporting timely and accurate information about agency operations, technology, and finances to the Legislature and the citizens of Montana.

To report fraud, waste, or abuse:

Online
www.Montanafraud.gov

Email
LADHotline@mt.gov

Call
(Statewide)
(800) 222-4446 or
(Helena)
(406) 444-4446

Text
(704) 430-3930

identifies critical processes and assets, however there are no defined strategies explaining how to regain those things in case of a disruption.

Continuity Training and Testing Is Not Thorough. While having a BCP documented is helpful, it lacks effectiveness if it hasn't been tested and staff are not aware of the overall procedures. Lottery does not have a program to effectively train or test their internal BCP that manages all office functions. They do test the production gaming backup system twice annually. However, the backup system testing was put on hold between October of 2019 and July of 2021 during the pandemic.

RECOMMENDATIONS:

In this report, we issued the following recommendations:
To the Lottery: 5
To the legislature: 0

Recommendation #1 (page 13):
Contract Management
Lottery needs to clearly define security requirements and the contractual tools to enforce them.

Lottery response: Concur

Recommendation #2 (page 18):
Cyber Supply Chain Management
Lottery needs to review the roles and activities of contractors and subcontractors and identify appropriate means to assure an effective structure of control throughout Lottery's supply chain.

Lottery response: Concur

Recommendation #3 (page 24):
Testing Acceptance Plan
Lottery needs to ensure legal requirements of sports betting and system functionality align and formalize testing plans and procedures to avoid inconsistencies in future gaming service changes.

Lottery response: Concur

Recommendation #4 (page 27):
Business Continuity Management
Lottery needs to define policy and procedure for continuity management that address the administrative details and recovery strategies of business functions.

Lottery response: Concur

Recommendation #5 (page 29):
Business Continuity Plan Testing and Training
Lottery needs to include testing and training in continuity management so personnel are informed and the effectiveness of the plan and recovery strategies can be tested.

Lottery response: Concur

Chapter I – Introduction, Scope, and Objectives

Introduction

The Montana State Lottery (Lottery) was created in 1987 and has contributed significant funds to various state programs and the General Fund. Lottery is overseen and advised by a commission. The governor appoints five members to the commission to oversee Lottery operations, set policy, and determines games. The governor also appoints a lottery director.

Lottery is allocated to the Department of Administration (DOA). While DOA manages Lottery's budgeting and reporting and represents Lottery in communications with the governor, Lottery manages other required agency activities such as hiring and maintaining staff.

The Lottery offers various types of online games and scratch tickets, such as Powerball, Montana Millionaire, Treasure Play, and Sports Betting. These games are determined and managed by Lottery, with gaming services, software, and hardware provided by various contractors. However, Lottery uses one primary contractor, Intralot, for providing most services. Intralot has various locations across the United States but have dedicated staff assigned to Montana Lottery within Helena. The contractor systems support main lottery operations including random number generators, independent verification of lottery operations, and the newly established Sports Bet Montana system. Each of these systems is described below.

Lottery Operating System (LOTOS): LOTOS is the overall system that provides separate applications that run the main functions of Lottery. These include:

1. Central Gaming System (CGS): This is the system that manages all online games including game settings, data processing, reporting, and telecommunications with retailers. This system communicates with all Lottery terminals in the field through a closed, encrypted, secure satellite and cellular network.
2. Orion: This new system supports sports betting services and is part of the contractor's CGS/LOTOS system. Just like online games and tickets, sports betting consists of terminals located at approved retailers for one-time wagers. However, there is also a phone application for players to establish an account for repeated play. This allows a person to create an online account, deposit money, and pick bets at any time. The application also only allows a person to officially place and pay for wagers when the phone is located within a licensed retailer though. All aspects of the phone application are managed by the contractor through a new system, Orion. Orion is used to manage sports betting account set up, maintenance, operation, and financial transactions.
3. Back Office System (BOS): BOS is the administrative part of CGS and is used for administrative tasks like reporting, inventory tracking, and managing retailers and gaming terminals.
4. Instant Game Management System (IGMS): IGMS is the application that is used for tracking inventory and activity of scratch tickets.

Random Number Generators (RNGs): Lottery also uses RNGs for the Montana Lottery's lotto style games. A certified RNG is used for Montana Millionaire, Big Sky Bonus, and Montana Cash games.

Internal Control System (ICS): ICS independently processes the same data as CGS to verify results including online draws, balancing sales, and winners. This system is meant to be separate from CGS. Therefore, to manage it, a subcontractor is hired by the primary contractor in coordination with Lottery.

In addition to the systems that support lottery games, there are systems that support Lottery's operations and security as well.

Badge Access System: This system maintains physical security at all doorways within the Lottery building in Helena through a multi-factor authentication system with both a physical key card and code.

Camera System: These cameras monitor physical activity inside and outside Lottery's building.

Ticket Verification System: A separate workstation is also maintained by the security department to perform security checks for winning tickets. This check includes verifying the activity of the ticket through the ticket barcode.

Sports Bet Montana Established in March 2020

Sports Betting is the act of playing a wager on the outcome of a sporting event. Until a few years ago, it was mostly illegal across the United States. A New Jersey Supreme Court decision in 2018 spurred federal action on legalizing sports betting and states have been developing legislation to legalize the activity since then.

Montana passed legislation in 2019 that added legalized sports betting to existing lottery statutes. Sports betting introduces a new aspect of management due to how it allows players to pick bets and place wagers. Therefore new administrative rules were also created to define legal sports betting activity and management.

All gaming aspects of sports betting are managed by Intralot as an additional service under the existing contract. An amendment to the contract was signed on March 6, 2020, to further define how sports betting would be implemented and managed between them and Lottery.

Lottery's Contractor Relationships Are Becoming More Complex

Lottery's direct service relationships are seemingly simple, with Intralot supplying and managing the central gaming system and support systems. There is also a separate contractor, Scientific Games, supplying scratch tickets and the State Information Technology Services Division (SITSD) providing basic infrastructure for office operations like email, desktop software, and phones, as well as network connectivity such as firewall management, router maintenance, and security scanning.

However, when looking at Intralot's services, multiple subcontractors are also involved in supporting these services. The significant services provided by subcontractors identified during our audit include:

- Independent validation of lottery operations,
- Verification of location and age for sports betting accounts,
- Software on tablets used by sales representatives, and
- Payment processing for the sports betting application.

New Digital Services Increase the Size of Cyber Supply Chains

A cyber supply chain refers to the processes, systems, networks, and technology used to provide a service or product to an organization. In recent years, cyber supply chains have become complicated due to organizations increasing reliance on multiple levels of suppliers to increase efficiency. Cyber supply chains now consist of direct contractors and multiple layers of subcontractors that provide a wide range of services.

As organizations continue to expand digital services, work environments, and products, the size and complexity of the supply chain can become immense. The introduction of sports betting and new technologies has increased Lottery's cyber supply chain and therefore, increased the risks needing to be managed by Lottery.

Audit Scope and Objectives

The Legislative Audit Division is required by §23-7-411, MCA, to review the following 18 areas as part of a security audit every two years.

These areas were assessed for risks and existing safeguards. Our assessment including evaluating risks specific to Lottery in each of the 18 areas, identifying what controls currently exist to mitigate those risks, and determining the level of impact and likelihood the risk has to Lottery operations with the identified controls already in place. Table 1 (see page 4) includes the summary of assessment work for each review area within statute at the time of planning the audit. As part of our assessment of risk, we assigned a rating to denote if significant, moderate, or minimal potential risk still existed after controls were applied.

Table 1

Audit Risk Assessment Results for the 2020 Lottery Security Audit

Required Statue Areas	Rating		
	High	Medium	Low
Personnel security		✓	
Lottery sales agent security	✓		
Lottery contractor security		✓	
Security of manufacturing operations of Lottery contractors			✓
Security against ticket or chance counterfeiting and alteration and other means of fraudulently winning			✓
Security of drawings among entries or finalists	✓		
Computer security	✓		
Data communications security			✓
Database security	✓		
Systems security	✓		
Lottery premises and warehouse security	✓		
Security in distribution	✓		
Security involving validation and payment procedures		✓	
Security involving unclaimed prizes			✓
Security aspects applicable to each particular lottery game			✓
Security of drawings in games whenever winners are determined by drawings			✓
The completeness of security against locating winners in lottery games with preprinted winners by persons involved in their production, storage, distribution, administration, or sales		✓	
Any other aspects of security applicable to any particular lottery game and to the Lottery and its operations	✓		

Source: Compiled by the Legislative Audit Division.

As required by statute, the last area of review include various other aspects of IT security. Therefore, we included general IT assessment work as it related to Lottery operations. The summary is shown below:

Table 2
General IT Assessment Areas for the 2020 Lottery Security Audit

Assessment Area	Description	Rating		
		High	Medium	Low
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.			✓
Topic of Interest	Represents any interest from the Legislature, the public, or other audit work.	✓		
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.	✓		
Impact of System Failure	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.		✓	
Management/ Governance	Defined by the structure, oversight, and management procedures the department has related to the topic/ system.		✓	
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.		✓	
Nature and Profile	Defined by the complexity, age, and cost of a system; number of users and levels of security within a system; criticality of system operations; sensitivity of the information processed; and the reliance on decisions a system executes.	✓		

Source: Compiled by the Legislative Audit Division.

Throughout the assessment, three common themes appeared among the high-risks areas:

- Lottery relies heavily on contractors and subcontractors to provide services for Lottery operation. Controls are needed to manage third-party contracts and agreements to maintain security and integrity of gaming operations. While DOA provides services, their services are excluded from the scope of this audit due to the larger operation of maintaining the state network for all agencies, not just Lottery.
- Sports betting introduced new applications, new procedures, and new legal requirements for the system. Controls are needed to ensure the changes made meet legal requirements and the new application is operating as required and expected.

- Both DOA and contractors provide services to Lottery. Therefore, details and coordination between these entities need to be specific and understood to ensure that disruptions to any services are minimized.

Based on the identification of these risks, the following objectives were developed for the audit:

- Determine if third-party assurances are scoped to ensure the integrity and security of Montana State Lottery operations.
- Determine if Montana State Lottery manages sports betting accounts according to state law and rule to ensure authorized play and payout occur.
- Determine if Montana State Lottery has continuity planning protocols to minimize organizational disruptions.

Audit Methodologies

Third-party assurance audit methodologies included:

- Working with Lottery to understand what hardware assets exist to support the software and gaming system network.
- Reviewing and identifying the contractors' or service providers' ownership and responsibility over maintenance.
- Reviewing contracts and other agreements to identify what security assurances and maintenance requirements exist.
- Identifying if current assurances include critical data and operations to ensure security requirements, security best practices, and guidance are met.
- Contacting other states' lotteries as part of identifying guidance and best practices specific to receiving contractor assurances.

Sports betting account management audit methodologies included:

- Identifying sports betting account management requirements within law and rule.
- Reviewing how the system is expected to meet these requirements by conducting interviews with Lottery staff and reviewing sports betting terms and conditions.
- Reviewing system testing to identify if legal requirements for sports betting account management is included.
- Reviewing contractual agreements for testing new sports betting functionality.
- Testing system functionality for restricting ineligible player accounts.
- Identifying if ineligible players were allowed to create sports betting accounts and place bets/wagers.

Business continuity plans and management audit methodologies included:

- Gathering criteria regarding Montana State Lottery continuity plan requirements and any standards or guidance offered by DOA.
- Reviewing Lottery and contractor continuity plans to understand what procedures, systems, situations, and individuals are involved.

- Identifying Lottery's involvement with the contractor's continuity plan and Lottery's awareness of the contractor's role in the plan.
- Comparing the continuity plans to the identified criteria to determine whether the plans are current, tested, and meet standards.

We also compared various processes to industry standards to identify where they can be strengthened to better ensure the integrity of Lottery security. Industry standards used included:

- National Institute of Standards and Technology (NIST): Provides a catalog of security and privacy controls for information systems. Montana state policy requires the use of NIST as guidance for security risk management and has established baseline security controls from NIST.
- Control Objectives for Information and Related Technology (COBIT): Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks.
- North American Association of State and Provincial Lotteries (NASPL): This association represents 53 lottery organizations in North America and provides guidance, communications, and training to lotteries.

Prior Audit Work

The previous Lottery security audit included eight recommendations. These recommendations focused on risk assessments, security policies and procedures, and access management. Lottery has hired an Information Systems Security Officer (ISSO) to manage the implementation of audit recommendations. Our follow-up work found that four recommendations were implemented, one recommendation is being implemented, and three recommendations are partially implemented. While progress has been made, overall, core concepts are still being established. The structure of security governance, including policies and procedures for physical security, logical system access, and activity tracking, has been strengthened. More work on defining security roles with the new ISSO and maturing the risk assessment process is being done.

Implementing an effective risk management framework can be a substantial task. However, having a defined and established risk management process allows an organization to recognize and address potential threats before they become a problem. While Lottery has made progress to the previous issued recommendations, we still advise work continue to make improvements. Further improvements to the risk assessment process identified in the follow-up work include removing potential conflicts of interest or undue influence and inefficiencies introduced by an unclear segregation of duty. A formalized and well-defined risk assessment process would not only identify and address potential of the afore mentioned threats, but also identify the root cause of a problem and prevent these problems from appearing again. See Appendix A for further details on the status of each recommendation.

Report Contents

While Lottery has made progress implementing risk management procedures since the last audit, there are still key areas being developed that need more attention. Our work this cycle identified the need for more visibility and accountability for contractors within the cyber supply chain of Lottery's services. We

identified the need to improve testing plans when new functionality or services have legal requirements that need to be made as well as better management of continuity planning. The following chapters discuss our findings and recommendations to Lottery:

1. Chapter II – Cyber Supply Chain Risk Management
2. Chapter III – Sports Betting Implementation
3. Chapter IV – Business Continuity Management

Chapter II – Cyber Supply Chain Risk Management

Introduction

As supply chains grow, visibility and control over the data flow within the supply chain shift from the central organization. Due to the decentralization, the risk of attacks grows exponentially.

With the introduction of sports betting and new digital services for identity and location verification, Montana State Lottery (Lottery) is gaining efficiency and increasing services. However, if these subsequent services of the supply chain were compromised, Lottery could ultimately be at risk of personal data loss, such as bank or credit card information, or issues with system operating integrity. As the provider of the final product, Lottery is responsible for ensuring the security of their cyber supply chain. While having control over security at various subcontractors is not feasible, there is guidance available to help organizations like Lottery in these situations.

Recent Best Practices Developed to Help Manage Cyber Supply Chain Risks

Due to the increase in supply chain attacks in recent years, research has been conducted to develop key practices that can help reduce cybersecurity risks within a supply chain. The National Institute of Standards and Technology (NIST) has been gathering information since 2015 on the surge in supply chain attacks to develop recent and relevant best practices.

From this guidance, core practices can be used to set a foundation that more in-depth and advanced practices can be built on. For instance, if the organization isn't completely aware of the data and infrastructure accessible by subcontractors, they aren't going to be able to establish useful security assessments for contractors.

An organization first needs to know what data and infrastructure is accessible or managed by subcontractors throughout the entire supply chain. This information is crucial in assessing where risk to the supply chain is high and further control is needed.

After a thorough understanding of the supply chain is established, the owner of the supply chain needs to gain more control and visibility into the high-risk areas of the supply chain. This is to understand controls and get assurance that risks outside of their direct control are managed. Once there is more visibility into the supply chain, the organization then needs to firmly manage commitments and agreements to ensure security requirements are being met and enforced.

There are specific practices that can be used depending on the amount of risk, resources, and expertise of the organization. While some practices would not be efficient or necessary in Lottery's situation, such as establishing councils or teams to review supply chain risks, there are key practices for smaller organizations, such as:

1. Creating explicit processes for supply chain and cybersecurity functions.
2. Increasing executive board involvement in cyber supply chain risk discussions and performance.

3. Clearly defining roles and responsibilities for contractor relationships and contract management.
4. Clearly stating security requirements in contractual agreements with contractors based on risk associated with the contractor.
5. Request the same security requirements for subcontractors.
6. Identifying reportable metrics that allow the organization visibility into the contractor's processes.
7. Using third-party assessments, site visits, and certifications to assess critical contractors.

State policy mirrors a key practice from this guidance which is the need for stronger contractual agreements. It requires the following specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk:

- System configurations or functionality align with necessary security standards,
- Security-related documents, such as security plans, exist, and
- Necessary assurances or evaluations of security are defined.

The following sections discuss our work in understanding Lottery's basic practices in managing supply chain risks. It discusses our review of current supply chain and cybersecurity controls and assurances.

Current Security Requirements Are Not Being Met

Strong contractual agreements with clear and enforced security requirements are critical to managing supply chain risks. Lottery is currently under contract with the primary contractor for Lottery operations and gaming systems until 2025. To identify security requirements related to the services from the contractor, we reviewed the contract, request for proposal, contractor response, and any amendments since the contract was initiated in 2016.

The standard contract with the main gaming contractor has a single statement for noncompliance with Department of Administration (DOA) policy. It states that DOA can modify or cancel any contract, project, or activity not in compliance with state Information Technology (IT) policy. While this is vague, the standard contract does refer to the Request for Proposal (RFP) and response as contractual agreements where additional security requirements can be listed.

Lottery's gaming operations RFP has multiple statements about the required security of the system they are seeking, and the contractor commits to meeting those requirements if selected. However, our work identified that the contractor has not supplied this information to Lottery as needed.

Security Planning: The RFP specifically asks for a detailed security plan. The contractor's response states a complete plan will be provided prior to the system being implemented. While the response provides a thorough overview of the security plan sections, Lottery has not received a security plan for the upgraded gaming system that was installed in 2016.

Subcontractors: Subcontractors involved in Lottery's system need to also be identified by the contractor and approved by Lottery. The RFP states the contractor will also provide a certificate of some manner stating the subcontractor is following the same security standards as the contractor. We identified five subcontractors involved in Lottery operations. Lottery has not received notarized certification of security from any of the subcontractors involved in Lottery gaming operations. When we requested the information during fieldwork, Lottery did provide a security audit report from the identity verification contractor. However, the report was not sent as part of the contract requirements.

Securing Remote Access: The RFP requires certain risk analysis practices within the contractor's controls to secure any type of remote access into Lottery systems. These analysis practices identify various vulnerabilities, including network penetration and social engineering attacks. The practices should also include testing the resiliency of the contractor if an attack were to occur. Currently, third-party penetration testing is conducted, and Lottery was able to provide that report. However, the scope of the testing does not include social engineering tests.

Business Continuity: The RFP also requires a formal plan outlining how operations will continue if any interruptions occur. Lottery requires the plan to include 11 aspects of business continuity and that the plan be updated and provided to Lottery twice annually. This requirement allows Lottery to have an up-to-date understanding of what to do in a disruption. Significant changes in the contractor's business or structure could impact the plan. Lottery needs to know what changes to expect if a plan is activated and to trust the contractor is managing business continuity effectively. When we received the most recent business continuity plan, we identified changes made after the audit request. These changes were in reference to sports betting, which was implemented in March of 2020.

The plan covered most of the required aspects from the RFP, but was missing the following sections:

- Plan Validation, Testing, and Maintenance
- Software/Hardware Inventory Lists
- Personnel Access Matrix
- Network and Firewall Diagrams

Continuity Testing: Validation and testing of this plan is also a standard requirement and included in the contract. Lottery is responsible for planning and initiating the tests. In the past, Lottery and the contractor conducted failover testing, which ensures Lottery can continue computer and network operations in the event of a disruption or critical equipment failure. The last failover was conducted in October of 2019. The delays in testing and Lottery not receiving an updated plan after the implementation of sports betting indicate that regular maintenance of the business continuity plans is not being performed by the contractor as required.

Backup Services: The RFP also states that the contractor will provide a backup of Random Number Generators (RNGs) which is housed at the contractor's facilities. It states that Lottery chooses which facility houses the RNGs and the contractor will ensure the RNGs have the same security controls as the production gaming system. Currently, the contractor has backup RNGs for Lottery, however, they are housed within the same physical location. Lottery also has a separate contract for draw services with the Multi-State Lottery Association that offers these back up services free of charge.

Contract Management Procedures Need to Be Strengthened

Cyber supply chain risk management includes strong contract management practices. One of the key best practices for securing the cyber supply chain is to monitor and enforce security requirements. However, Lottery has been passive in enforcing the current requirements of the contract. Lottery indicated they work through problems when they arise in a forward-looking manner. Lottery stated that the mission and direction has always been to generate revenue for the state. Lottery has not spent enough time assessing contract provisions with Intralot.

The lottery contract includes various tools for managing situations where the vendor is not meeting specific contract provisions. However, they are vague when trying to apply them to the situations identified during the audit.

The contract references multiple types of liquidated damages including failure to meet physical and system security requirements. Lottery and the contractor agree that certain types of activity by the contractor could delay or disrupt Lottery operations, but the exact amount of damages is not clear. Liquidated damages relative to security requirements discuss incidents and establish a liquidated damage of $1,000 per incident per day.

The contract also defines situations when one or more parties are not honoring a contractual agreement within the breach of contract clause. It is standard for contracts to have statements defining what a breach looks like for each party and what actions should be taken if a breach is identified. In Lottery's contract, the breach definition includes the failure to submit any report required by the contract.

These contract provisions are for severe or extreme cases, which may not apply to the findings of the audit. However, if a security breach of some sort occurred that could have been mitigated by these security requirements, the situation may become severe or extreme. These contract provisions are an opportunity to work with the contractor to ensure they are meeting the needs of Montana, and if they do not clearly address security, Lottery has the option to amend the contract with language that is more specific.

Lottery Needs to Define Security Requirements and Enforce Them

It appears Intralot has not provided information noted in the breach of contract sections and they are not meeting system security requirements covered in liquidated damages sections. However, all of the specific security requirements are scattered throughout a document that is over 800 pages and tools for enforcing these requirements are not clearly stated or defined.

If security is to be taken seriously by the contractor and any subcontractors, Lottery needs to determine how to address the situations we identified and establish stricter contract management procedures. Security requirements and enforcement tools cannot be ambiguous within the contract or buried within large, unmanageable documents. Otherwise, they become a burden to manage and enforce, and require Lottery and Intralot staff to spend unnecessary time interpreting and monitoring.

While the main focus of Lottery's business is generating revenue for the state, it is crucial for the integrity of the game as well as increasing revenue to ensure that data and operations are protected

from fraudulent or malicious behavior. This behavior could occur at any level of the supply chain and ultimately impact Lottery operations or the personal data of those who play Montana Lottery games.

RECOMMENDATION #1

We recommend that Montana State Lottery:

A. *Clearly define necessary security requirements and tools to enforce them in a Security Exhibit or Addendum within the current contract.*

B. *Actively manage the security requirements.*

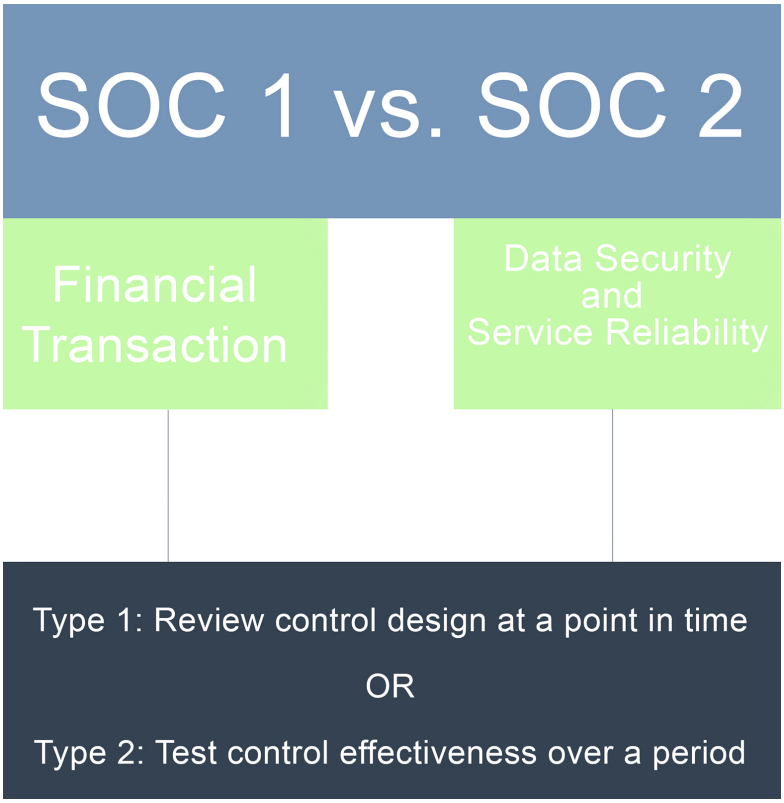
Third-Party Security Assurances From Critical Service Providers

Key practices discuss the need for enforcing security requirements and maintaining accountability for contractors, while also recognizing that an organization may need flexibility in how this is completed. For higher risks, it may be necessary to conduct their own audits or test contractor operations if an organization has the means to do so. For organizations that do not have the staff or resources to do so, a third-party is often hired to provide assurances that the organization needs.

Obtaining assurances from a contractor can come from various types of reports, but most often are in the form of third-party, independent audits known as Service Auditor Reports or System and Organization Control (SOC) audits. The objectives of the assurances should be based on the needs of the customer and defined during the contracting process. The audit firm then completes the work and provides the report to the customer. Reputable audit firms conduct this work in accordance with audit standards and can use various industry standards, such as Trust service criteria from the American Institute of Certified Public Accountants (AICPA) or the National Institute of Standards and Technology (NIST).

These assurances can come in various forms and can provide different benefits for organizations. There are two common SOC reports and each report can have two types. The following figure (see page 14) shows the most common SOC reports and describes the difference between the four common SOC reports. Lottery receives a SOC 1, Type 2 report, from Intralot.

Figure 1
Common SOC Report Descriptions



Source: Compiled by the Legislative Audit Division.

Lottery Currently Receives Various Audit Reports

Lottery requires the systems offered need to comply with NIST's common criteria, national lottery best practices, international security standards, world lottery security control standards, and Multi-State Lottery Association (MUSL) requirements. In response to this requirement, Intralot states that various audits are conducted as a measure to ensure security as well as discusses security governance and practices within their security governance.

Intralot provides Lottery a SOC 1 Type 2 report on a yearly basis. This report focuses on the contractor's control structure in place that mitigates any risks that could adversely affect Lottery financials. There are 28 control areas tested, including, but not limited to, organizational and administrative, software development and changes, access controls, computer operations, ticket validations, prize validations, reporting, and billing.

Lottery also receives a similar report from Scientific Games that provides scratch tickets to Lottery. Lottery receives a third-party assessment of the contractor specific to the operations they provide to Lottery. While this isn't a SOC report, this audit is from an independent organization and addresses relevant risks to Lottery operations. The objectives of the audit are to assess the adequacy of controls that ensure security, integrity, honesty, and fairness of scratch-tickets developed by the contractor. The audit firm conducting the assessment also reviews control effectiveness by testing a sample of tickets over a period. The most recent report was issued in May 2019 and it reviewed a sample of tickets from the prior 12 months. Because this contractor provides lottery tickets to multiple states, the objectives and scope of this work is a shared agreement between the states and the auditing firm. Each state gets an individual addendum as part of the report if something specific to their state is identified.

As part of our work to understand how these reports provide lottery visibility into the supply chain and assure security and integrity of operations, we reviewed the scope and testing methodologies for these reports. The following sections discuss how these reports are beneficial but also fall short in assuring security of the contractor and subcontractor operations.

Current Security Assurances Do Not Cover Critical Cybersecurity Risks

While these reports provide Lottery assurances to some contractor operations, like scratch tickets and financial transactions, they do not provide assurances that would reduce cybersecurity risks to all of Lottery operations.

- The scratch ticket contractor provides a thorough report of their operations and control structure, but this report is limited to only a portion of Lottery's business.
- The SOC 1 report from the gaming system contractor covers a few aspects of IT, but it is only those that would impact transactions and financial statements.

SOC 1 reports are directed at control objectives. A control objective is a set of controls at a service organization (contractor) to address risks to a user entity's (organization or customers) internal control over financial reporting. Whereas, SOC 2 reports are directed at trust service criteria relevant to a contractor's services, operations, and compliance. Trust service criteria includes best practices and industry standards in areas of security, confidentiality, availability, privacy, and processing integrity.

Table 3 (see page 16) shows how certain aspects of a SOC 2 report can be covered in a SOC 1, but a large portion of controls are not within the scope of the SOC 1, Type 2 report Lottery currently receives.

Table 3
SOC 1 & 2 Coverage Comparison

Description of SOC 2 Controls Tested	Comparison to Lottery SOC 1
Security Control environment, communication, risk assessment, monitoring, logical and physical controls, system operations, change management, risk mitigation.	Control objectives identify if security policies are in place, annual security training occurred, procedures exist, and application access security exists. *It does not review risk management and mitigation, change management, system configuration, vulnerability or patching, incident response procedures, or access controls beyond applications.*
Availability Processing capacity planning and monitoring, environmental protections, recoverability of systems and data.	Capacity planning is not addressed in the control review. The SOC 1 identifies environmental safeguards and data replication procedures but *does not review capacity planning and management or recovery procedures and business continuity.*
Processing Integrity Policy/procedure to ensure quality, accuracy, reliability of data, storage is accurate and complete.	These controls are not directly tested similarly. However, due to the nature of information and processing by the contractor, many of the financial controls tested would cover processing integrity.
Confidentiality Information is identified, classified, protected and disposed of properly.	Confidentiality is only mentioned concerning HR data and ensuring employees take a confidentiality training yearly. *The standard controls for data confidentiality are not yet tested.*
Privacy Communication, choice and content, collection, use, retention, access, disclosure of private information. Quality and monitoring of private information.	Privacy is only mentioned concerning ensuring employees take a privacy training yearly. *The standard controls for data confidentiality are not tested.*

Source: Compiled by the Legislative Audit Division.

When reviewing the scope of each report, we also identified that neither of these assurances discuss subcontractors or provide assurance over subcontractor operations and security. This is common for these types of assurance reports and increases the need for thorough supply chain risk assessment and coordination with direct contractors.

Other States Require Various Security Assurances

Other states use similar contractors and services, so the situation and risks are comparable to Lottery. We contacted other lotteries to identify what assurances they receive to mitigate the same risks.

Eleven states were contacted, seven of which are using the same contractor as Montana. Seven states responded, five states using the same contractor and two others. The states were asked to share what kind of assurance reports were received, if subcontractors were included, and if there were contractual requirements for the reports. Table 4 shows the response information received from other states.

Table 4
Montana Compared to Other States Contractor Assurance Information

State	Soc 1 (Type 2)	Soc 2 (Type 2)	Additional Assurance	Contract Requirement	Subcontractors Included
Montana	✓				
Washington	✓	✓	✓	✓	✓
Idaho	✓			✓	
Wyoming	✓			✓	
Colorado	✓		✓	✓	✓
New Mexico	✓		✓		
Louisiana		✓	✓		
New Hampshire		✓		✓	

Source: Compiled by the Legislative Audit Division.

In most cases, other states receive a SOC 1 Type 2 report; however, a few states have requested further assurance with a SOC 2 Type 2, security assessments, or cybersecurity audits. All of the states we contacted have contractual requirements for these assurances which vary in specificity. In contrast to Montana, most states clearly state requirements for general assurance within contract language. Furthermore, Colorado, Washington, Idaho, and New Mexico have requirements in the contract for the lottery to approve the audit firm, approve the assurance objectives, or even require the lottery to manage all audit communications. These types of practices are used to reduce the risk of biased work and ensuring the audit firm maintains independence from the contractor.

Lottery Needs to Continually Assess Supply Chain Risks and Identify Appropriate Assurances

A key practice for managing cyber security risks in a supply chain is the use of third-party assessments, such as SOC reports or other specific audits from independent entities. While Lottery receives third-party assurance through the SOC report from Intralot, it is not clearly stated as a requirement in the

new contract from 2016. Lottery management indicated third-party assurance was specifically required in the previous contract, but not in the current contract. Intralot has continued to send the SOC reports as assurance every year to Lottery. While the current contract indicates Intralot has third-party assurances, it does not explicitly request them or discuss what they should be assuring.

While it's important to use these reports when an agency can't directly test controls, obtaining these assurances without having a clear connection to some kind of risk can create a false sense of security. If Lottery assumes the vendor is managing these risks, they may not develop appropriate controls on their side of the business, which in turn could allow risks to go unidentified. This passive approach to managing security requirements and analyzing risks leaves Lottery reacting to issues instead of proactively addressing the risk landscape as it changes.

For Lottery, it's more important to establish basic practices of identifying the data flow and infrastructure that supports services and consistently update that information as systems change or new services are provided. Once this is done, Lottery can methodically determine what security requirements should be in place for contractors and subcontractors and how they want to gain assurance that cybersecurity risks are mitigated.

As Lottery continues to provide more gaming options, such as sports betting, they have had to increase their reliance on a contractor to maintain efficiency. This gives the contractor control over all sports betting activity and management, including gathering personal information, processing payment transactions, and managing how Montana law and rule are upheld within gaming operations. Critical risks in any of these areas could cause loss of personal data or impact the integrity of Lottery operations.

RECOMMENDATION #2

We recommend Montana State Lottery improve cyber supply chain risk management by:

A. *Reviewing the role and activity of each contractor and subcontractor,*

B. *Identifying appropriate assurances, and*

C. *Strengthening contractual agreements to require appropriate, ongoing assurance.*

Chapter III – Sports Betting Implementation

Introduction

Sports betting gives players the ability to place wagers on outcomes of various sport activities. In the 2019 Legislative Session, House Bill 725 was passed legalizing sports betting within Montana. The Montana State Lottery (Lottery) worked to define rules to regulate sports betting shortly after. Lottery chose to amend the current gaming contract to include sports betting as an additional service from the contractor that already provides this service to other states.

Sports Bet Montana began in March 2020. Players place wagers at licensed facilities through an application downloaded on their phone or directly at a terminal. Players also have the option to pick wagers through an online website to generate a barcode that can be used to place wagers directly at a terminal in a licensed facility.

Sports Betting Offers New Technology and Systems

When sports betting was introduced, it was added to current legal regulations for Lottery restrictions and licensing. However, sports betting needed further restriction and licensing regulations based on how it is managed. These additional restrictions are related to mobile gaming which involves money transferring or active wagering.

Sports betting account activities are defined in law and Lottery promulgated new administrative rules to implement current restrictions. The rules define restrictions that prevent illegal activity such as money laundering or one person running multiple sports betting accounts. The new procedures are intended to manage sports betting accounts in a way that ensures they are legal, and the integrity of sports betting is maintained.

To provide the sports betting service, a new application was introduced to Lottery's overall gaming system. This application, called Orion, manages sports betting accounts, allows players to pick bets, as well as deposit and withdraw money through a subcontracted payment service provider. The main gaming system contractor manages Orion completely and provides Lottery access to view reports related to sports betting financials, investigate wagers, and individual player accounts.

Sports Betting Requires Player Account Management

Because new technology is used to provide the online services of sports betting, the systems involved need to help Lottery meet these legal requirements. General information technology (IT) account management concepts also apply to player account management within sports betting. Account management reduces the risks identified above and maintains the integrity of the game. Sports betting administrative rule aligns with these general concepts in the following ways:

Identify and Authenticate: Identifying each user in a system enables an agency to hold each user accountable for their actions. Assigning a unique identification to every user allows tracking on who's taking which specific actions in a system. Authentication ensures that whomever is accessing a system is who they say they are. For sports betting, these concepts ensure that a player's activity is their own

activity and they are not impersonating anyone to play. For example, a contractor cannot pretend to be a nonrestricted player when establishing a sports betting account. Along with needing to be an eligible player, rule also states that only one account is allowed per person, the person must be 18 years or older, and the person cannot be a part of any self-exclusion program.

Monitor: Once authentic activity is identified and documented, a process to monitor that activity needs to be in place to ensure the activity is authorized. For sports betting, this concept would be in place to monitor accounts for fraudulent activity. While not defined explicitly in rule, unauthorized or illegal activity is most often related to multiple accounts owned by one person or a group of individuals colluding to manipulate the game's odds or help a person to win. As stated in rule, fraudulent activity specific to online accounts also includes transferring of money between individual accounts but can also include the overuse of chargebacks to refund player's debit cards.

Remediate: If unauthorized activity is identified, actions need to be taken to stop the activity and prevent further harm to an organization. This concept addresses how sports betting accounts would be managed after such activity is identified. Rule states that Lottery may suspend accounts with:

- Illegal activity,
- Fraudulent or multiple failed money deposits,
- Inactivity for 18 months,
- Violation of terms and conditions, or
- If the account was issues in violation of statute or rule.

Rule also explains restricted activity of suspended accounts, how to restore an account, and when and how funds can be withdrawn from accounts.

New Services Need to Meet Legal Requirements

Even though Lottery does not have management responsibilities over the system, they are still accountable for ensuring sports betting occurs in accordance with legal requirements. Due to the limited control Lottery has over this system and account management, it's important they work closely with the contractor to ensure the system is meeting legal requirements.

Audit work included reviewing testing procedures and results to identify specific account management activities. Some functionality, such as restricting ineligible players from creating accounts, was tested in the system as well. We also reviewed the sports betting website's terms and conditions to identify how the system should act in specific situations.

The following sections discuss our review of how these activities are controlled and how Lottery ensures the system is meeting legal requirements when managed completely by a contractor.

Ensure Legal Requirements of System Are Tested

It is best practice to ensure a system is validated against legal and contractual requirements before final implementation. This validation happens through various levels of testing. Lottery relies on the

contractor for most of this testing. The contract amendment further defining the services for sports betting establishes testing responsibilities. It clearly states the contractor will conduct quality assurance testing and provide a user acceptance testing environment for Lottery. This is a common separation of testing responsibilities as it makes sense for the contractor to test the functionality of the system to requirements and the customer to test the system in reference to business processes they manage.

Lottery also has national guidance noted in the gaming system contract for Lottery and the contractor to follow. While the national guidance is from 2004, the practices still align with updated industry standards. The guidance and industry standard both include developing a test plan based on the risks of the system changes or upgrades and needs of the business. The plan should include what testing needs to be completed and by whom, what the process is to address issues, how testing will be considered complete, and clear metrics for an acceptable product.

The testing plan should include detailed test cases to direct testing activities and document outcomes. These are important to ensure specific functionality is addressed, understand if it's working or not, and determine how to move forward when functionality isn't working as required. Management and stakeholders use this information to determine if new functionality should go into the live system. The contractor states in the response to the RFP that they use testing plans to meet all of these requirements and encourage Lottery to recommend test cases for the testing plan to ensure system functionality meets expectations and requirements.

New Service Does Not Meet All Legal Requirements

Various systems are used to manage sports betting, so multiple tests cases were created to test the specifics to Montana's sports betting needs. Lottery provided a spreadsheet of test cases conducted by the contractor for our review. After reviewing the testing, we were able to identify test cases for some of the account activity necessary to manage sports betting accounts and activity.

While test cases addressing some of the more basic functions were identified, there were others with no test cases. Furthermore, after reviewing the sports betting website, we identified activities from the website terms and conditions were not in agreement with rule. The following discusses the activities that were tested by Intralot.

Account Inactivity and Suspension: Test cases show accounts can be manually moved to blocked/suspended in case of fraudulent or illegal activity. Although there are three test cases related to suspension, there is an inconsistency between website terms and conditions and rule. The definition of inactivity in rule is 18 months of no bets being placed. Test cases indicate rule is correct and the system determines inactivity based on betting activity and not logins. However, website terms and conditions define inactivity as not logging in to the account for 18 months.

Another condition of suspending an account in rule is if a balance goes negative. Negative account balance suspensions were not included in any of the reviewed test cases. It's likely the system will not allow a player to place a bet for more money than is available. The remaining activity that would require an account to be suspended (fraudulent or multiple failed electronic deposits, account issued in error or violation of law, or it violates the terms and conditions of the website) are not addressed in test cases.

There doesn't appear to be a systematic way to track administrative rule provisions requiring Lottery to suspend a sports wagering account.

Suspended Account Activity: Test cases were identified that indicate withdrawals cannot be made by a player in a closed/suspended status. However, deposit, changing accounts, and deletion by a player are not addressed even though they are explicitly prohibited in rule.

Self-Exclusion from Sports Betting: There is an inconsistency with how rule describes self-exclusion procedures and how the system manages the process. ARM 2.63.1304 indicates signing up for this program requires an application be completed online. ARM 2.63.1301 also states that prior to establishing an account, Lottery has to ensure the player is not on the self-exclusion list. However, the actual process to self-exclude is to establish a sports betting account and then opt-in to the self-exclusion list through account options. While this is minor, it is further evidence that Lottery did not perform due diligence in reviewing the new operations being added to gaming.

Child Support Liens: The review of Lottery winnings for any liens is established in law. According to terms and conditions of the website, there is a Sports Wagering Winnings Intercept process to identify players owing child support. However, there were no test cases identified verifying this process was tested or works.

Ineligible Player Management: State law restricts certain individuals from playing the Montana Lottery. This includes employees, contractor staff, auditors, commissioners, and any household members for these groups. When an account is created, personal information such as name, a picture of a valid driver's license, address, and last four digits of the social security number are gathered to verify the player is a real person and does not already have a sports betting account. Even though the system validates individuals creating sports betting accounts, this validation is only to ensure age and identity. There were no test cases related to ineligible players creating sports betting accounts. It does not compare information against the restricted player information that Lottery maintains and uses to review lottery tickets. Audit staff were also able to create a sports betting account that was verified and ready to start placing sports wagers.

Lottery Needs to Engage in System Testing Procedures

Part of managing a system is ensuring it operates in line with business and legal requirements. While we understand the challenges of customizing contractor services such as sports betting, there needs to be a process in place to ensure legal requirements are being met. Currently, Lottery does not have a formal way to plan this interaction with Intralot to ensure the services they receive meet requirements.

Overall, there are areas where sports betting accounts are not acting according to law and rule. Additionally, there are areas where published website terms and conditions contradict or do not align with rule or actual functionality. Both of these situations can cause confusion over how the system functions for a player trying to understand rules and for a legislator trying to establish rules for acceptable gaming. In either case, the integrity of Lottery can be disrupted. Players going along with how the game directs them may not be aware of legal issues. For example, if an account is suspended,

rule indicates the player may not conduct certain activities. However, there's no assurance the system stops them from these activities.

After discussions with Lottery about ineligible players, they engaged with the contractor to find solutions during fieldwork. Lottery manually compared the restricted player list and sports betting accounts within the system. Through their review, Lottery identified another restricted player with an active account.

Since this was identified, Lottery has continued this manual review on a monthly basis. The contractor provides Lottery a report of potential matches between name, address, and the last four digits of social security number. Lottery then reviews the list to confirm duplicates and have accounts suspended. Lottery is also requesting the contractor create functionality to automatically complete this review.

Lottery also indicated a plan is in place to update rule with the specifics of how account management works in the new system to address the other inconsistencies identified.

Formal Testing Procedures and Documentation Needed for New Services or Significant System Changes

Lottery stated that they do not normally document their test cases of game changes, so they did not document testing for sports betting account management. Sports betting was not considered a new system. It is considered a new game, or service, in which the contractor completely manages. Therefore, Lottery did not view sports betting as an implementation that needed formal controls documentation for requirement discussions and testing.

These management decisions also provide information on how Lottery addresses two important risks:

- Risks introduced by functionality changes.
- Risks introduced by changing contractors or subcontractors in Lottery's cyber supply chain.

While the contractor may indicate formal testing procedures are carried out on their side, Lottery needs to make themselves more of a part of that process. This will help Lottery verify it is occurring and understand what risks are reduced or increased with each system change. When a system is maintained or, in Lottery's case, completely managed by a contractor, these test cases allow for visibility into the contractor's management procedures. However, it also requires Lottery verify some of this testing through their own acceptance testing. Through their own formal process, Lottery can ensure the new services being provided meet legal requirements, gain visibility into contractor operations to verify controls, and identify or update risks to their operations.

RECOMMENDATION #3

We recommend Montana State Lottery:

A. *Ensure changes are made that align the system functionality with legal requirements of sports betting account management.*

B. *Improve system testing procedures by identifying when a formal testing plan is needed and verify legal requirements are met by new functionality.*

Chapter IV – Business Continuity Planning

Introduction

Montana State Lottery (Lottery) relies on information systems to manage scratch ticket inventory, operate their online gaming, and sports betting. These systems are critical to Lottery operations. Disruptions to normal operations, such as fire, earthquake, pandemic, or cyberattack, could affect Lottery operations or systems and potentially mean a significant loss of revenue for the state. These organizational disruptions can be minimized through business continuity planning protocols. These protocols are documented in business continuity plans (BCPs) that outline how operations will be restored and continue during an unplanned disruption in service. Without these plans, Lottery would ultimately be at risk of lost revenue and potential loss of reputation and future business.

A BCP is a comprehensive plan that contains contingencies for business functions, assets, human resources, and business partners. Every aspect of the business that might be affected should be considered. As this is a critical process for Lottery and state government, the Department of Administration (DOA) provides the standards, procedures, guidance, and tools for establishing agency continuity plans.

State Requirements Exist for Managing Business Continuity

State security policy lists baseline controls for contingency planning. These controls include establishing policy and procedures, details of a BCP, testing the BCP, and business aspects that should be addressed in the BCP.

DOA has also outlined procedures for the development and maintenance of BCPs. They provide a template for agencies to ensure critical components are included and standardized in all BCPs, such as identification of services, resources, delegations of authority, and necessary contact information. DOA also stores the plans, but it is the responsibility of each agency to develop and manage the plan.

State policy also requires these plans to integrate with other government and non-government organizations that provide services. This integration is key when critical services are provided by contractors because additional coordination is needed to ensure continuation of services. There may also be penalties or damages that can be assessed for the services that are paid for, but not provided by the contractor as expected. For example, Lottery includes BCP requirements within the contract for the main gaming system. These requirements relate to the content of the BCP as well as coordination between Lottery and the contractor to test and revise the plan.

Currently Lottery has two BCPs that require some integration:

1. Lottery's internal plan addresses Lottery's office operations such as connecting to the state network or finding an alternate work site for staff.
2. Lottery runs the games on contractor-supplied hardware and software. The nature of the contractor's BCP is to provide multiple redundancies to that system to keep services available at all times.

Lottery's Internal Business Continuity Plan Is Missing Essential Details

When reviewing the BCPs, we focused on the primary purpose of a BCP, which is defining the essential business functions. These are the functions that enable an organization to provide vital services and sustain operations during a disruption. They can be summarized by three key attributes:

1. Identification of the essential business functions and their associated priority within the organization.
2. The acceptable amount of time to restore each function in a disruption.
3. The required assets, tasks, and strategies to restore each function within the acceptable amount of time, and how the assets are procured or where they are stored should also be defined in this process.

The BCP managed by the gaming system contractor was not missing any of the key attributes required in state policy. However, after reviewing Lottery's internal BCP, we identified areas where Lottery can improve management and training to ensure the continuity of critical operations.

Lottery's internal BCP identifies essential business functions, their associated priority, and their recovery time objectives, but there are no defined processes or strategies explaining how to achieve those objectives. For example, the restoration process that Lottery defines for each function simply states that duties will be assigned at the time of event. There is always potential for personnel absences during an event. If the personnel responsible for restoring an essential function are unavailable, processes do not exist for other personnel to restore the function. Specific instances of missing strategies identified in our work include:

- Lottery's internal BCP identifies the gaming system as a critical information system that needs to be running; however, it doesn't provide a person to contact during business interruptions.
- The entity or process for providing backup random number generating is not defined in the BCP.
- There is an alternate furnished facility for Lottery if the primary Lottery facility is rendered unusable. The internal BCP does not include a point of contact at DOA, what provisions are available, and how Lottery can access them.

Administrative details that show management of the internal BCP were also missing:

- No signoff date by the plan owner.
- No executive authority (overall responsibility for plan) listed.
- Outdated e-mail address for the contractor .

The Previous Internal BCP Met State Policy Standards

Lottery was able to provide an old BCP from 2008 that included this information during fieldwork. However, this BCP is inactive due to DOA's initiative to standardize and centralize BCPs across the

agencies. DOA is responsible for the Continuity of Operation/Continuity of Government (COOP/COG) and is the state's certifying authority for all COOP/COG plans. These responsibilities are in coordination with Montana Disaster and Emergency Services (DES) to ensure the continuity of state government during disruptions.

Due to this initiative, Lottery switched to the state's system and plan template in 2017. Lottery indicated they also depend on DOA to update their internal BCP. However, the updates provided are limited to DOA's monthly requests to ensure employee contact information is current. Some confusion exists as to whether Lottery was supposed to stop using their original plan after creating the state-required plan. DOA did not respond to auditor's requests for information on which direction Lottery should have taken or needs to go.

Policy and Procedure to Manage and Coordinate Business Continuity Is Needed

State security policy requires each agency have policy and procedures for contingency planning and that it is updated every two years. The agency's policy should define contents of the BCP, considerations to be addressed in the plan, and procedures to manage the plan–namely review, training, and testing.

While the direction from DOA's initiative may be unclear, in the past Lottery has completed thorough business continuity planning. They should use the state-required plan to further build on their current plan and develop internal policy and procedure to manage their plan. A formal process to manage the plan would ensure that Lottery's internal plan:

- Has complete administrative information and approvals.
- Contains complete and useful strategies to restore essential business functions to minimize organizational disruptions.
- Integrates with other BCPs to minimize operational disruptions.

RECOMMENDATION #4

We recommend Montana State Lottery create policy and procedure for managing, reviewing, and updating their continuity plan that ensures complete and useful information is present, including:

A. *Administrative details and contact information for all continuity personnel and third parties,*

B. *Clear definitions of essential functions and the strategy to restore each essential function, and*

C. *Documentation of critical information systems and assets required to restore each essential function, including how the information systems and assets are backed-up, procured, or stored.*

Training and Testing of a BCP Is a Critical Management Procedure

While a thoroughly documented BCP is critical to maintaining operations during disruptions, ensuring the plan works and meets the needs of the business is just as important. This is done through training and testing of the BCP. This requires the identification, training, and preparedness of personnel capable of performing continuity responsibilities.

Testing serves to assess and validate all the components of a business continuity plan and identify deficiencies for further improvement. Testing should be conducted annually and should go through the procedures necessary for:

- Activating necessary staff, facilities, and resources,
- Recovering vital records and information systems, and
- Testing interdependencies with other organizations.

Additionally, there should be a process for formally documenting and reporting tests and results. A debriefing should be conducted after each test for participants to identify deficiencies in the continuity plan and to recommend revisions to the plan. State policy and industry standards require these management practices be completed every year or when major changes to any business function occur.

BCP Training and Testing Is Not Thorough Enough to Ensure Continuity

Lottery does not have a program to effectively train or test their BCP. Training on the BCP is limited to the continuity personnel identified in the plan being informed of their responsibilities. There is no agency-wide continuity training or awareness. Training continuity personnel does not have to be rigorous but is important for successful recovery from a disruption. Personnel should be informed of their roles and responsibilities and understand the entire process for recovery and the steps required to successfully enact them.

Lottery's testing for business continuity is limited to failing the main gaming system over to the backup system every six months. Failover allows an organization to continue computer and network operations in the event of a disruption or critical equipment failure at the primary site. The information and communication systems specific to Lottery are duplicated at the contractor's facilities and all business transactions are mirrored on these systems.

While this may address a failure in the main gaming system, it doesn't address the coordination needed between other contractors and DOA services. The testing necessary does not have to be burdensome. Lottery could conduct a tabletop exercise where continuity personnel walk through the steps of their recovery procedures in a meeting. Functional exercises could be limited to testing critical IT infrastructure and failover capabilities with the contractor. Lottery could then document the results of these exercises and adjust the plan for any deficiencies identified in testing.

Failover Testing Was Not Conducted After Sports Betting Started

Failover tests between Lottery and their contractor are typically conducted every six months. Lottery is responsible for planning and initiating the tests and the contractor's testing program is adjusted when corrective action is necessary.

The last failover was conducted in October of 2019. Lottery stated the contractor did not supply updated BCPs and failover tests were not conducted due to the implementation of the new sports betting system. Lottery resumed failover testing in June 2021.

In addition to implementing sports betting, Lottery cited COVID 19 for the delays experienced in receiving updated BCPs and conducting failover testing. COVID 19 is a perfect example of why business continuity planning is important. It would ensure continuation of business operations and that regular testing can still occur during a pandemic.

Lottery Needs to Improve BCP Training and Testing Programs

Lottery needs a program in place to ensure the effectiveness of contingency efforts and to coordinate both the contractor BCP and their internal BCP. A BCP is only effective if it is complete, can be taught to personnel, and that personnel can test these processes. The program should include annual training, testing, and maintenance whenever services, systems, or business operations change.

The program also needs to include a review of the entire cyber supply chain as it changes or grows with new services. Lottery needs assurance that contractor services or Lottery operations will continue if a subcontractor service has interruptions. For example, Lottery needs to know backup plans are in place and effective if geolocation services are not available. These services ensure sports wagers are placed in licensed facilities and could stop sports wagering during key events if they are interrupted, which could reduce state revenue. Without understanding the continuity of subcontractors services, Lottery cannot plan for or anticipate what will happen if disruptions occur.

RECOMMENDATION #5

We recommend Montana State Lottery develop and implement a training and testing program in conjunction with their continuity plan such that:

A. *Personnel are formally informed of and trained on any roles and responsibilities they may have in executing the continuity plan.*

B. *Testing of the continuity plan be performed so that restoration of essential functions can be demonstrated.*

C. *The continuity plan is updated to address any deficiencies identified during testing program.*

Appendix A

Introduction

The *Lottery Security (18DP-02)* report was issued to the Legislative Audit Committee in September 2018. The audit included eight recommendations to the Montana State Lottery (Lottery). In April 2021, we conducted follow-up work to assess implementation of the report recommendations. The following sections summarize the progress toward implementation of the report recommendations.

Recommendation #1

We recommend the Lottery establish a risk management framework for information technology that aligns with state policy and industry standards.

Implementation Status: Being Implemented

Our initial audit work identified that Lottery does not have a defined Information Technology (IT) risk assessment process, leaving key IT security policies and procedures unestablished. Committing to a formalized risk assessment framework will help the Lottery better address threats to its IT infrastructure and effectively implement its organizational goals and objectives. Montana Lottery indicated that an IT risk management and assessment framework is being developed. As part of follow-up work, we reviewed the framework for key practices such as clear procedures, roles, and responsibilities, risk identification, and annual reviews and updates as operations change. Risk assessment procedure defines that the Security Director, Information Technology Director, and the Information Systems Security Officer will assess risks annually and that risk mitigation plans and progress will be updated quarterly until complete. The current risk assessment process exists as a spreadsheet with tabs for each of the different systems being assessed. However, an assessment has not been performed for the new sports betting system that was implemented in 2020. A repeatable, formal risk assessment process would have discussed the new risks for new systems or business procedures. Implementing the risk management framework properly is crucial as many of the findings identified in the initial audit stemmed from Lottery not having a formalized IT risk management framework. Lottery has not provided a timeline for final implementation of the framework but will continue to refine the documentation and process as changes are made to the Lottery systems.

Recommendation #2:

We recommend Lottery establish a process within the risk management framework that addresses the results of third-party assessments.

Implementation Status: Implemented

Lottery is subject to periodic evaluations from various third-parties, including the Legislative Audit Division, the Multi-State Lottery Association, and the Federal Bureau of Investigation. Our initial audit found the Lottery has not fully implemented recommendations made from these types of evaluations. Successful implementation of these recommendations ensures that Lottery can maintain continued operation, avoid penalties, and comply with state and third-party policy. As part of follow-up work, we identified that Montana Lottery compiled a detailed list of prior IT security audit findings and third-party assessments. Procedures were created to ensure that recommendations are understood, and steps

are taken until they are implemented. This procedure is documented and reviewed semiannually by the security director, IT director, and ISSO.

Recommendation #3:

We recommend Lottery:

A. Evaluate and modify job descriptions for the IT Director, Security Director, and Criminal Investigator to clearly define IT security duties.

B. Integrate Information Security Manager responsibilities among these positions or seek additional means to address any issues with separation of duties or conflicts of interest.

Implementation Status: Partially Implemented

Our initial audit identified that Lottery has not assigned IT security responsibilities in a way that ensures its IT security program aligns with state guidance and industry standards. Many gaps existed within the information security manager responsibilities that could lead to threats to IT security not being properly identified or addressed. Successful integration of security management responsibilities among those tasked with IT security would ensure that a successful security plan could be created, maintained, and enacted. Following the audit, Lottery defined these duties within policy and procedure when applicable to Lottery-specific operation rather than adjust job descriptions.

Lottery also hired an Information Systems Security Officer (ISSO) to absorb additional Information Security Manager (ISM) duties that were not already present in existing job descriptions or procedure. ISM duties are now shared by the Security Director, IT Director, and the ISSO with the intention that having the ISSO as a third-party would address any issues with separation of duties or conflict of interest. While the ISM responsibilities within Lottery are now addressed, there are overlaps in who is responsible for different aspects of security and potential conflicts of interest have been introduced. For example, the Security Director and IT Director are responsible for granting and recording access. They are also two of the three ISMs who perform Lottery access reviews. They are reviewing their own work, while the ISSO observes as a third-party. The ISSO is relatively new to Lottery and could be subject to undue influence from the department directors. Considering the nature of the Lottery, these conflicts of interest within IT security could lead to possible fraud or other forms of abuse.

For smaller agencies like Lottery, spreading ISM duties among multiple staff is an effective way to ensure that information security is effectively managed. Care must be taken to prevent conflicts such as efficiency versus security or reviewing one's own activity. If Lottery were to follow State guidance to implement an information security program and reassign ISM duties so that they do not overlap, there would not be a need for additional staff present when reviewing security controls and conflicts of interest would be addressed.

Recommendation #4:

We recommend Lottery:

A. Further develop and enforce required IT security policies and procedures that govern operations specific to Lottery.

B. Ensure those tasked with information security management are knowledgeable and trained in information security management principles.

Implementation Status: Implemented

Our initial audit identified that policies and procedures for IT security specific to Lottery operations were not present and that IT security training for those managing security needed improvement. Security standards and state policy require well-defined policies and procedures as part of an effective security program. These policies alone do not make an effective program. Lottery also needs security management staff that are adequately trained to be capable of securing Lottery specific operations. Following the audit, Lottery developed new policies and procedures that govern the security of their unique IT environment. The ISMs are responsible for enforcing and measuring compliance with the newly-developed security policies. The IT director also developed three new cybersecurity training programs to ensure that those tasked with managing information security are informed of emerging security threats. Lottery states the training programs will be updated for relevancy as necessary.

Recommendation #5:

We recommend Lottery establish access control policies and procedures that encompass all systems including:

A. Defined, documented procedure for granting, approving, changing, and removing access.

B. Periodic, documented user access reviews.

C. Complete documentation of current access of each user within each system.

D. Documented access level expectations for each user within the system.

Implementation Status: Implemented

Our initial audit found that access management to various Lottery systems was limited and not governed effectively. By not having defined procedures to govern access, there is no assurance that user activity within the Lottery's computer systems is valid or authorized. This could lead to security issues including, but not limited to, access to critical gaming system code, security systems, and personal information. Since the audit, Lottery has created well-defined access management policies and procedures that encompass all Lottery systems. For all systems, there is a defined, documented procedure for granting, approving, changing, and removing access. Critical system access is reviewed daily while others are reviewed semiannually. Examples of these completed reviews were provided by Lottery and examined as part of our follow-up work. Documentation of current access of each user within each system is now also maintained by staff, as well as their associated access level expectations.

Recommendation #6:

We recommend Lottery improve access management by:

A. Developing policies and procedures that enforce least privilege and segregated access for both internal and contractor staff.

B. Reviewing current contractor staff access and limiting privileged access.

C. Identifying and documenting privileged roles and any security requirements for those roles.

D. Clearly defining segregations for all systems, information security duties, and any additional controls required due to personal relationships within Lottery.

E. Including review of least privilege and segregation of duties when periodically reviewing access.

Implementation Status: Partially Implemented

Initial audit work identified certain user roles that had questionable logical access and segregations of duties were not clearly defined. By establishing policies and procedures that ensure least privilege access is enforced and segregation of duties are defined, Lottery has a better chance at preventing unauthorized access and can more easily identify if it occurs. As part of follow-up work, policies and procedures were identified that clearly define how least privilege and segregated access is enforced and reviewed, which addresses the first three elements of this recommendation. Follow-up work further identified policy to address security threats due to personal relationships within Lottery and procedures that clearly define segregation of access and duties for all systems. The ISMs periodically reviews access and least privilege, however, the unclear segregation of duties among the ISMs has the potential to introduce conflicts of interest or undue influence.

Recommendation #7:

We recommend that Lottery improve user activity tracking by:

A. Ensuring individual user accounts and profiles are used on all workstations and systems including requirements for individual user accounts when establishing access management policies and procedures.

B. Defining auditable events regarding all systems, databases, and physical locations.

C. Ensuring complete and accurate auditing or logging is available, secured, and reviewed relative to the risk associated with each auditable event.

Implementation Status: Implemented

The initial audit identified several instances of shared user accounts and access to workstations that were not secured with individual user accounts. Without access controls in place, it is not possible to monitor and analyze unlawful, unauthorized, or inappropriate activity. Enforcing individual user access to all systems is necessary to ensure the actions of unique users can be traced for accountability purposes. Since the audit, Lottery has implemented policies and procedures for access management. All systems now require individual credentials for access and the systems have defined auditable events related to use and access. Certain auditable events on critical systems are reviewed daily while others are reviewed semiannually.

Recommendation #8:

We recommend Lottery increase physical security by:

A. Conducting and documenting analysis with the state chief information officer to determine the most secure location for servers.

B. Establishing and updating physical access policies and procedures regarding high-risk IT areas.

C. Establishing procedures for consistently monitoring physical access to alert or detect unauthorized access.

Implementation Status: Partially Implemented

Our initial audit identified that IT systems critical to Lottery operations were housed internally where access was not always limited to only those with a need to work with those systems. Considering the importance of these IT systems, unauthorized physical access to these systems could interfere with the integrity of the entire Lottery. As part of follow-up, Lottery has indicated that the state Chief Information Officer has granted Lottery an exemption allowing Lottery to keep the Internal Control System (ICS) and Random Number Generator (RNG) servers in Lottery and vendor operated facilities. The exemption we received, however, is not current and Lottery has not responded to our request for a current exemption. If Lottery doesn't keep this exemption current, it could influence SITSD to change their stance on the exemption and interrupt Lottery operations while the servers are migrated to the state data center.

Lottery has updated physical access policies and procedures regarding high-risk IT areas. They have moved critical servers to a more secure area where staff cannot access the servers without proper approvals. Other physical security improvements were made and controls to track that access have been implemented – these include alarmed motion sensors, physical locks on servers, door locks requiring badge and code, magnetic door counters, and internal and external cameras which record the door counter.

Montana State Lottery

Lottery Response

September 30, 2021

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

RECEIVED
October 1, 2021
LEGISLATIVE AUDIT DIV.

RE: Response to the 2020 Montana State Lottery Security Audit

Dear Mr. Maciver:

Thank you for the opportunity to respond to the report on the Montana State Lottery Security Audit, dated September 24, 2021.

The Montana Lottery concurs with the audit findings and will take the necessary action to comply with all recommendations. In addition, security and information technology staff will conduct a review of the actions taken with Legislative Audit staff to ensure the issues are being properly addressed.

The following is our response and action plan to the specific recommendations of the audit:

RECOMMENTATION #1

We recommend Lottery:

A. **Clearly define necessary security requirements and tools to enforce them in a Security Exhibit or Addendum within the current contract.**
B. **Actively manage the security requirements.**

The Montana Lottery concurs with this recommendation and will combine all IT Security language from all Lottery Operating System contract documentation to create a single point of reference to be used by the Lottery and vendor to enforce contract requirements. Additionally, IT Security Requirement Enforcement policy, procedure and sign-off review forms will be finalized to ensure the vendor is complying with all IT security requirements. IT security administrators will also periodically review and maintain this documentation to ensure future potential risks are also addressed as identified.

RECOMMENTATION #2

We recommend Montana State Lottery improve cyber supply chain risk management by:

A. **Reviewing the role and activity of each contractor and subcontractor,**
B. **Identifying appropriate assurances, and**
C. **Strengthening contractual agreements to require appropriate, ongoing assurance.**

The Montana Lottery concurs with this recommendation and will include the identification and review of all vendor subcontractor IT security assurances per audit finding and NIST recommendation. Periodic review of subcontractors utilizing Cyber Supply Chain Risk Management recommendations with contractual obligations clearly identified will help ensure Lottery is properly addressing the recommendation.

RECOMMENTATION #3

We recommend Montana State Lottery:

A. **Ensure changes are made that align the system functionality with legal requirements of sports betting account management.**
B. **Improve system testing procedures by identifying when a formal testing plan is needed and verify legal requirements are met by new functionality.**

The Montana Lottery concurs with this recommendation and will review and align sports betting Rule, Lottery MCA, and sports betting terms & conditions to ensure language is consistent across all channels. Sports betting test cases specifically based on Rule, MCA, and terms & conditions will also be finalized and used regularly to ensure continued compliance with current legal requirements.

RECOMMENTATION #4

We recommend Montana State Lottery create policy and procedure for managing, reviewing, and updating their continuity plan that ensures complete and useful information is present, including:

A. **Administrative details and contact information for all continuity personnel and third parties,**
B. **Clear definitions of essential functions and the strategy to restore each essential function, and**
C. **Documentation of critical information systems and assets required to restore each essential function, including how the information systems and assets are backed-up, procured, or stored.**

The Montana Lottery concurs with this recommendation and will update Lottery (BCP) Business Continuity Plan documentation to include key resources for essential business functions. Additionally, Lottery BCP responsibilities policy, procedure, and review forms will include all essential business function information; including role, available resource, assets required, and restoration strategy.

RECOMMENTATION #5

We recommend Montana State Lottery develop and implement a training and testing program in conjunction with their continuity plan such that:

D. **Personnel are formally informed of and trained on any roles and responsibilities they may have in executing the continuity plan.**
E. **Testing of the continuity plan be performed so that restoration of essential functions can be demonstrated.**
F. **The continuity plan is updated to address any deficiencies identified during testing program.**

The Montana Lottery concurs with this recommendation and will formalize, improve, and document a Lottery Business Continuity Responsibilities policy, procedure, and review form. This documentation will include responsible personnel for the execution of BCP plans and their respective roles. The BCP plan will be periodically reviewed, and tabletop tested to ensure it is current and accurate. Updates to the plan will be made as deficiencies are identified during review and testing, and those issues are resolved.

Thank you again for the opportunity to respond. We look forward to maintaining a good rapport with your team and look forward to working with them in the future.

Sincerely,

Scott Sales, Director

Montana Lottery

Audit Recommendation	Lottery Response	Corrective Action Plan	Responsible Area	Target Date
RECOMMENTATION #1 **We recommend Lottery:** **A. Clearly define necessary security requirements and tools to enforce them in a Security Exhibit or Addendum within the current contract.** **B. Actively manage the security requirements.**	Concur	1A • Analyze and extract all IT security language from Lottery operating system RFP, vendor response, Lottery operating system contract, and accompanying documentation to create a single point of reference for all IT security requirements. This reference will be used by the Lottery and vendor to enforce requirements. • Future Lottery Operating System contracts will include this specific single point of reference for all IT security requirements. 1B • An IT Security Requirements Enforcement policy, procedure, and sign-off review form will be created and managed by the Lottery Information System Security Officer to ensure the vendor is complying with requirements. • IT security administrators will also periodically review policy and procedure with the Lottery Director to ensure vendor compliance as well as ensuring all newly identified, potential emerging IT security risks are being addressed. *Policies, procedure, and forms impacted (current and new)* *IT Security Requirements Enforcement Policy* *IT Security Requirements Enforcement Procedure* *IT Security Requirements Enforcement Review Form*	MT Lottery IT (primary) MT Lottery ISSO	Mar – 22 Mar – 22
RECOMMENTATION #2 **We recommend Montana State Lottery improve cyber supply chain risk management by:**	Concur	2A • The action plan for recommendation 1 includes the creation of IT Security Requirements Enforcement management documentation. This documentation will also include the	MT Lottery IT (primary)	Mar – 22

A. Reviewing the role and activity of each contractor and subcontractor, **B. Identifying appropriate assurances, and** **C. Strengthening contractual agreements to require appropriate, ongoing assurance.**		necessary C-SCRM (Cyber Supply Chain Risk Management) data as per audit finding and NIST recommendation. All vendor subcontractors will be defined per C-SCRM recommendation. 2B • Per C-SCRM recommendations subcontractor role, access granted, and IT security assurance verification will be defined and reviewed periodically to ensure continued compliance. 2C • The IT Security Requirements Enforcement management documentation will also include reference to the contractual obligations as defined in the Lottery operating system contract to ensure continued compliance is achieved. *Policies, procedure, and forms impacted (current and new)* *Sub-section of IT Security Requirements Enforcement Policy, Procedure, and Review Form*	MT Lottery ISSO MT Lottery ISSO	Mar – 22 Mar – 22
RECOMMENTATION #3 **We recommend Montana State Lottery:** **A. Ensure changes are made that align the system functionality with legal requirements of sports betting account management.** **B. Improve system testing procedures**	Concur	3A • Examine and align sports betting Rule, Lottery MCA, and sports betting terms and conditions. Update where necessary to ensure language is consistent across all channels. 3B • Create test cases based on Rule, MCA, and terms & condition requirements and execute those test cases regularly to ensure compliance with all legal requirements defined. *Policies, procedure, and forms impacted (current and new)*	MT Lottery IT (primary) MT Lottery IT	Mar – 22 Mar – 22

by identifying when a formal testing plan is needed and verify legal requirements are met by new functionality.		*Sports Betting legal requirement Test Cases*		
RECOMMENTATION #4 **We recommend Montana State Lottery create policy and procedure for managing, reviewing, and updating their continuity plan that ensures complete and useful information is present, including:** **A. Administrative details and contact information for all continuity personnel and third parties,** **B. Clear definitions of essential functions and the strategy to restore each essential function, and** **C. Documentation of critical information systems and assets required to restore each essential function, including**	Concur	4A • The Lottery (BCP) Business Continuity Plan will be complimented with the creation of IT security policy, procedure, and review forms to ensure the BCP is complete and current moving forward. • The Lottery Business Continuity Plan will be updated to include key resources for essential business functions. 4B • Essential business functions included in the Lottery Business Continuity Plan will be clearly defined with instructions on how to contact those resources to restore those functions. 4C • As mentioned in 4B the essential business functions will be documented; including the assets needed to perform those business functions. *Policies, procedure, and forms impacted (current and new)* *Lottery Business Continuity Plan Responsibilities Policy* *Lottery BCP Management Procedure* *Lottery BCP Review Form*	MT Lottery Security (primary) MT Lottery ISSO MT Lottery ISSO	Mar – 22 Mar – 22 Mar – 22

how the information systems and assets are backed-up, procured, or stored.				
RECOMMENTATION #5 **We recommend Montana State Lottery develop and implement a training and testing program in conjunction with their continuity plan such that:** **A. Personnel are formally informed of and trained on any roles and responsibilities they may have in executing the continuity plan.** **B. Testing of the continuity plan be performed so that restoration of essential functions can be demonstrated.** **C. The continuity plan is updated to address any deficiencies identified during testing program.**	Concur	5A • As noted in response to recommendation 4, a Lottery Business Continuity Responsibilities Policy, Lottery BCP Management Procedure and Lottery BCP Review Form will be formalized. Included will be key personnel responsible for the execution of BCP plans and their respective roles. 5B • BCP documentation will also include the periodic review and tabletop testing of the plan to ensure the BCP data remains current, and the plan remains accurate. 5C • Any deficiencies identified during the BCP review and tabletop testing will be documented within the Lottery BCP Review Form to ensure all issues are resolved, and respective BCP plan document is updated.	MT Lottery Security (primary) MT Lottery Security MT Lottery ISSO	Mar – 22 Mar – 22 Mar – 22