Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology

Governor's Office of Information Technology

Audit of Cybersecurity Resiliency

Public Report

May 2023

Report Number 2250P-IT

Eide Bailly LLC

EideBailly®

CPAs & BUSINESS ADVISORS

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Senator Robert Rodriquez
Chair

Representative Andrew Boesenecker

Representative Gabe Evans

Senator Rhonda Fields

Representative Lisa Frizell
Vice Chair

Representative Dafna Michaelson Jenet

Senator Rod Pelton

Senator Kevin Van Winkle

OFFICE OF THE STATE AUDITOR

Kerri L. Hunter, CPA, CFE	State Auditor
Cindi Radke, CISA	Contract Monitor
Eide Bailly LLP	Contractor

REPORT NUMBER 2250P-IT

EideBailly®

CPAs & BUSINESS ADVISORS

May 2023

Members of the Legislative Audit Committee:

This report contains the results of the Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology. The audit was conducted pursuant to Section 2-3-103, C.R.S, which authorizes the State Auditor to conduct audits and assess the security practices of information technology systems of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology.

We conducted this performance 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 findings and conclusions based on our audit objectives.

During our audit work, we identified certain matters that were considered sensitive to protecting state information technology assets. Accordingly, these matters are not included in this report but were reported to the Governor's Office of Information Technology management in a separate confidential report dated May 2023.

E. Anders Erickson
Principal, Risk Advisory Services
Eide Bailly, LLC

CONTENTS

REPORT HIGHLIGHTS

Audit of Cybersecurity Resiliency at the Governor’s Office of Information Technology
IT Performance Audit, May 2023 – Report Number 2250P-IT

AUDIT CONCERNS

Audits that conclude on an organization’s cybersecurity resiliency, can improve their ability to prevent, detect, and respond to cyber threats, which helps to minimize the risk and potential impact of security breaches, which in turn would increase the integrity of information systems and the associated data. Evaluating and improving the State’s cybersecurity posture directly relates to the Colorado General Assembly’s determination and declaration established in Section 24-37.5-401, C.R.S. Specifically, the General Assembly stated that the state government has a duty to the Colorado’s citizens to ensure that information the citizens have entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction [Section 24.37.5-401(b)].

By statute, the Governor’s Office of Information Technology (OIT) is responsible for delivery of information technology to State agencies, including the oversight and direction of information security, as well as ensuring that State agencies within the Executive Branch have established resilient cybersecurity practices and proper internal controls to identify, prevent, and detect cyber threats. This public report identifies the following main concerns:

- OIT has not clearly defined state-wide security roles and responsibilities to align with those same responsibilities outlined in Colorado Revised Statutes. This ambiguity has led to inconsistencies in the implementation of security practices and confusion on who is responsible for execution of security control activities – either OIT, an agency, or 3rd party vendor.
- OIT recently updated the Colorado Information Security Policies (CISPs) without proper education and planning to all affected parties. This lack of education has exacerbated the security roles and responsibilities issue as these updated policies migrated significant responsibilities from OIT to agencies.

Additional concerns were identified related to the areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access Controls, Risk Management, Security Planning, User Account Management, and Vulnerability and Patch Management. Due to the sensitive nature of these concerns, the details have been included in a separate, confidential report, as Findings 3 through 12.

BACKGROUND

The Governor’s Office of Information Technology

- OIT is the State’s centralized information technology department responsible for managing information technology resources and staff for all consolidated agencies.
- OIT is responsible for maintaining the State’s IT Security Program and managing the CISPs.

KEY FACTS AND FINDINGS

- OIT had not clearly defined OIT's security roles and responsibilities to align with those outlined in Colorado Revised Statutes.
- OIT had not established an effective and holistic approach for the prioritization of information systems across the State's IT enterprise.
- OIT had not effectively communicated the release of updated security policies to those who were responsible for their implementation and execution.
- OIT had not established minimum security requirements for key security activities.

Additional key facts and findings were identified related to the areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access Controls, Risk Management, Security Planning, User Account Management, and Vulnerability and Patch Management. Due to the sensitive nature of these key facts and findings, they have been included in a separate, confidential report, as Findings 3 through 12.

The box below provides a count of the total recommendations made from this audit, including those in both the public report and the associated confidential report. This box also provides a count of the number of recommendations with which OIT management agreed, partially agreed, or disagreed.

Recommendations Made

77

Responses

Agree: **56**

Partially Agree: **16**

Disagree: **5**

CHAPTER 1
OVERVIEW

Organizations perform cybersecurity resiliency audits to evaluate the strength and effectiveness of their cybersecurity measures and to identify vulnerabilities and potential weaknesses in their systems. Cybersecurity resiliency audits help organizations identify potential security gaps, whether they arise from outdated software, unsecured network devices, or inadequate security policies. This enables organizations to take proactive measures to address vulnerabilities and enhance their overall cybersecurity posture. Additionally, these audits can identify whether the organization is compliant with relevant laws, regulations, and industry standards, and whether they are adhering to their own internal security policies and procedures. By performing a cybersecurity resiliency audit, organizations can improve their ability to prevent, detect, and respond to cyber threats, which helps to minimize the potential impact of security breaches and protect their reputation. Ultimately, a cybersecurity resiliency audit is a critical tool for organizations to ensure that they are properly managing and mitigating the risks associated with cyber threats.

Governor's Office of Information Technology

The Governor's Office of Information Technology (OIT or the Office) is the State's centralized IT department responsible for managing IT resources and service delivery for state agencies that have been consolidated under statute [Section 24-37.5-102, C.R.S.]. OIT oversees executive branch department technology initiatives and recommends strategies to maximize service delivery efficiency, in a cost-effective manner, through the application of enterprise technology solutions. The Office provides services to consolidated agencies on a cost reimbursement basis with OIT acting as a vendor. The term "consolidated agencies" refers to all the departments, divisions, commissions, boards, bureaus, and institutions in the executive branch of the state government except for the following: Legislative Branch agencies; Judicial Branch agencies; the Departments of Education, Law, State, and Treasury; or state-supported institutions of higher education. [Section 24-37.5-102, C.R.S.] These agencies are also referred to as non-consolidated agencies. Services provided by OIT include enterprise application management and support, database management, network security and management, communication technology services, data center operations, information security, help desk services, public safety communications, procurement, project management, and IT economic development.

Audit Objectives, Scope, and Methodology

We conducted this performance audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of the state government. Audit work was performed from July 2022 through April 2023, and we appreciate the cooperation and assistance provided by the agency's management and staff.

We conducted this performance 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 findings and conclusions based on our audit objectives.

The key objectives of the audit include the following: (1) provide an independent assessment of the adequacy of OIT's cybersecurity practices; (2) identify areas for improvement, if any, that could enhance the security and resilience of Colorado's critical IT systems and infrastructure; and (3) ensure compliance with Colorado State law *Section 24-37.5-106, C.R.S.,* which outlines OIT's duties and responsibilities, as well as the duties of the Chief Information Officer.

To accomplish our audit objectives, we performed numerous auditing activities and utilized various sampling techniques. These activities and sampling techniques are outlined in each individual finding within the report.

As required by auditing standards, we planned our audit work to assess the effectiveness of those internal controls that were significant to our audit objectives. Details about the audit work supporting our findings and conclusions, including any deficiencies in internal control that were significant to our audit objectives, are described in the remainder of this report. Any details, including any deficiencies that could expose the overall state's cybersecurity posture are included in a separate, confidential report. Specifically, Findings 3 through 12 are included in a separate, confidential report, and address deficiencies we identified in the areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access Controls, Risk Management, Security Planning, User Account Management, and Vulnerability and Patch Management.

The scope and methodology of this cybersecurity resiliency audit utilized the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to assess the effectiveness of OIT's cybersecurity practices. The audit focused on OIT's ability to identify, protect, detect, respond to, and recover from cybersecurity events. Specifically, the audit evaluated OIT's compliance with the following five core functions as outlined in the NIST CSF:

- **Identify** – The organization's ability to identify and manage cybersecurity risks and vulnerabilities.
- **Protect** – The organization's controls to safeguard against cyber threats.
- **Detect** – The organization's capability to detect and respond to cybersecurity incidents in a timely manner.
- **Respond** – The organization's ability to respond to cybersecurity incidents to minimize the impact of the event.
- **Recover** – The organization's ability to restore normal business operations after a cybersecurity incident has occurred.

Additionally, the audit evaluated OIT's cybersecurity governance, risk management, and compliance with relevant laws, regulations, and industry standards. The audit also included the review of OIT's incident response plan, business continuity plan, and disaster recovery plan to determine whether they are up-to-date and effective.

A draft of this report was reviewed by OIT. Obtaining the views of responsible officials is an important part of ensuring that the report is accurate, complete, and objective. We, along with the Colorado Office of the State Auditor (OSA), were responsible for determining whether and how to revise the report, if appropriate, based on OIT's comments. The written responses to the recommendations and the related implementation dates were the sole responsibility of OIT. However, in accordance with auditing standards, we have included an Auditor's Addendum to responses that are inconsistent or in conflict with the findings or conclusions or do not adequately address the recommendations.

Unresolved Audit Recommendations

Since OIT's creation in 2008, the OSA has performed numerous audits and evaluations of OIT and the consolidated agencies and systems it supports. Many of these audits and evaluations, over the years, have identified ongoing, recurring issues leading to an accumulation of unresolved IT risks, associated with IT governance and security of the State. Recurring, unresolved audit and evaluation recommendations related to IT security that persist for years can be indicative of systemic issues with an organization's cyber resiliency. This table provides an analysis of where recommendations identified in past OSA reports are similar to problems identified in this latest cyber resiliency report.

			Access Management	Asset Management	Contingency Planning	Identification and Authentication	Incident Response	IT Governance	Logging and Monitoring	Physical Access Controls	Risk Management	Security Planning and Assessment	Security Training and Awareness	Vulnerability and Patch Management
Report Name	**Report Date**	**Number of Recommendations**	**Recommendations Similar to Problems Identified in this Report**											
Report on Controls Placed in Operation and Tests of Operating Effectiveness	Sep 2009	14	✓		✓	✓		✓	✓					✓
SAP Information System, Department of Transportation	Jun 2010	15	✓		✓	✓	✓					✓	✓	
Office of Cyber Security	Dec 2010	204		✓		✓	✓	✓						✓
Evaluation of the Sustainability of the Colorado Financial Reporting System	Jul 2011	2						✓						
Consolidation of Executive Branch Information Technology	Mar 2012	12	✓					✓						
Systems Backup and Recovery	Nov 2014	17	✓		✓	✓		✓			✓			
IT Vulnerability Assessment	Dec 2014	10	✓		✓	✓		✓						
Audit of the Info Security of the Colorado Operations Resource Engine System	Jun 2016	25		✓	✓									✓
Audit of Three Information Technology Systems at the CDPHE	Sep 2017	48	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓
Evaluation of State IT Resources	Dec 2018	52	✓					✓						
Procurement Process for Major Information Technology Projects	Mar 2019	21						✓						
Evaluation of Information Technology Security at CDOT	Feb 2020	49	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓
Information Technology Service Management	Mar 2022	10						✓						
Statewide Financial, Compliance, and Single Audit	2011 - 2021	369	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓
TOTAL RECOMMENDATIONS SINCE JULY 1, 2008		**848[1]**												

Source: *OSA Recommendations Database*

[1]The OSA tracks a recommendation with multiple subparts as multiple recommendations. For example, a recommendation with subparts “A” through “C” is tracked as three recommendations.

CHAPTER 2

PUBLIC FINDINGS AND INFORMATION

Finding 1: Governance and Oversight

The Chief Information Officer (CIO) is the state executive who leads the Governor's Office of Information Technology (OIT) and is ultimately responsible for the security of state systems and information *(Section 24-37.5-106, C.R.S.)*. As of July 1, 2008, Colorado State law required the consolidation of much of the state's IT resources, personnel, and equipment under OIT. This consolidation effort included the IT personnel and IT equipment previously residing within most executive branch departments, excluding the State's institutions of higher education.

The Chief Information Security Officer (CISO) within OIT reports to the CIO and serves as the point of contact for all information security initiatives in the State of Colorado, informing the CIO and executive agency leadership on security risks and impacts of policy and management decisions on IT-related initiatives *(Section 24-37.5-403, C.R.S.)*. The CISO leads OIT's Office of Information Security (OIS), which includes offices for IT Governance & Cybersecurity, Security Architecture, and Security Risk & Compliance. In addition, the CISO has oversight of the budgets for the OIT Security Operation Center (SOC) team and Identity and Access Management team. The OIS is responsible for developing and maintaining state security policies [including the Colorado Information Security Policies (CISPs)] and providing leadership for state security initiatives.

Agencies establish a Business Owner for each IT system. The Business Owner has a key role in the implementation and management of security for an individual system. The CISPs state that, "The Agency or entity that is the Data Steward is the Business Owner. The Business Owner has the authority to authorize or deny access to the data, and is responsible for the accuracy, integrity, and timeliness of the data." The role and responsibilities of Business Owners expanded significantly with the most recent version of the CISPs, which were released in March 2022. With these latest CISPs, OIT has shifted the majority of security related decisions to the Business Owners.

OIT has not consistently or clearly used the term "Business Owner" – *see problem 4 below*. To avoid confusion, throughout this report, where this term is intended to refer to an individual designated by OIT as their primary point of contact for the system at an agency, we have indicated this as "Business Owner (individual)".

What audit work was performed and what was the purpose?

To conduct our assessment and support our conclusions, we conducted interviews with OIT management and staff and a selection of staff within a sample of five consolidated agencies to understand the policies and practices in place for governance and oversight. Specifically, we:

- Compared OIT and CISO policies, procedures, and practices to the CISO roles and responsibilities, as outlined in Colorado Revised Statute.
- Analyzed the strategies and methods OIT has established to prioritize systems.

- Evaluated the processes and procedures for the release, communication, distribution, and review of CISPs and OIT Technical Standards.
- Examined roles and responsibilities for information security across OIT and the five selected consolidated agencies and compared these to actual activities taking place.
- Assessed the security roles and responsibilities for the fifteen selected systems across five selected consolidated agencies.

The purpose for the audit work performed was to evaluate OIT's design and implementation of control activities related to its governance and oversight of the State's information security activities, and the impact on OIT's cyber resiliency.

What problems did the audit work identify, how were the results measured, and why did they occur?

We identified the following problems at OIT regarding governance and oversight, along with why the problems occurred:

1. The CISO has not clearly defined OIT's security roles and responsibilities to align with those outlined in Colorado Revised Statutes. Through the CISPs, OIT has defined its roles and responsibilities as those of a service provider to consolidated agencies. However, the role of a service provider is inconsistent with the breadth of OIT's responsibilities as outlined in Colorado Revised Statutes.

   The March 2022 version of the CISPs define OIT's role as a service provider to State agencies and, in fact, the role OIT assigns themselves in these CISPs is that of an IT Service Provider (ITSP). The following are definitions of a "Service Provider" from several leading organizations in the Information Technology industry:

   > *A managed service provider (MSP) delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in the MSP's data center (hosting), or in a third-party data center. – Gartner (www.gartner.com)*
   >
   > *An organization responsible for managing and delivering services to another organization, as per their requirement, is called a managed service provider (MSP). Traditionally, an MSP was used to manage or deliver information technology (IT) services like infrastructure, security, networking and applications. – Forbes (www.forbes.com)*

   In these definitions, the **key** attribute of a service provider is that they **deliver services**. This delivery role is at the heart of the relationship between a service provider and its customers.

   However, while OIT's role does have a delivery component, the Colorado Revised Statutes that establish the role of a State-wide CISO and outline their duties and responsibilities *(Section 24-37.5-403, C.R.S.),* does not focus on or even mention service delivery. Consider the following excerpts of duties and responsibilities for the CISO from this statute *(bold added for emphasis)*:

- **Develop and update** information security policies, standards, and guidelines for public agencies.
- **Promulgate rules** containing information security policies, standards, and guidelines.
- **Ensure the incorporation of and compliance** with information security policies, standards, and guidelines.
- **Direct information security audits and assessments** in public agencies in order to ensure program compliance and adjustments.
- **Establish and direct a risk management process** to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.
- **Approve or disapprove and review** annually the information security plans of public agencies.

The required activities for OIT described in statute, as noted above, are not consistent with the role of a service provider. This misalignment of roles and responsibilities is further illustrated in the table below, which lists common IT security activities. The checkmarks identify where we either typically find each activity to be the responsibility of a Service Provider or Internal IT Department. The shaded cells represent where, based on our understanding, OIT has defined their role. Where the checkmarks and shaded cells are not aligned, there is greater risk of ownership not being defined and security activities not being implemented or conducted effectively and/or in compliance with statute.

IT Security Activity	Service Provider	Internal IT Department
Perform vendor oversight		▨ ✓
Create and manage information security policies		▨ ✓
Perform risk assessments		▨ ✓
Develop security awareness training material	▨ ✓	▨ ✓
Ensure security awareness training is received by all users	▨	✓
Perform or initiate audits of user access	▨	✓
Define or enforce minimum audit log requirements	▨	✓
Require all users to sign an Acceptable Use Agreement annually	▨	✓
Ensure individuals are screened prior to authorizing access to information systems	▨	✓
Ensure all organizational units have a continuity of operations plan	▨	✓
Establish and maintain an inventory of active user accounts	▨	✓
Manage physical access to IT assets	▨	✓
Perform vulnerability scans	▨ ✓	▨ ✓
Establish and test incident response plan		▨ ✓
Establish and test a disaster recovery plan		▨ ✓

Throughout our audit, OIT has provided mixed responses on its role as an IT Service Provider vs. an IT department for consolidated agencies. Multiple times, OIT personnel stated they are simply a service provider that provides IT services to agencies and that OIT is not responsible for whether agencies follow or comply with CISPs.

OIT has not provided an explanation for why they have not formally agreed upon their role. Throughout conversations with OIT they have stated that, at the end of the day, it is up to the agency to comply with CISPs and any regulations that may apply to the agencies' information systems. However, as described above, Colorado Revised Statutes state that the CISO shall ensure the compliance of all CISPs, and if a control or service is not being managed by OIT, OIT still has the responsibility to review and ensure the controls are in place to protect the State's data and resources.

Section 24-37.5-401(1)(e), C.R.S., states that information security policies must be implemented throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and resources that support the operations and assets of those agencies.

Section 24-37.5-403(2)(c and d), C.R.S., states that the CISO shall (c) ensure compliance with information security policies in the information security plans developed by public agencies and (d) direct information security audits and assessments in public agencies in order to ensure compliance and adjustments.

Standards for Internal Control in the Federal Government (Green Book) Principle 14.3 states that management should communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. In these communications, management assigns the internal control responsibilities for key roles.

2. OIT had not established an effective and holistic approach for the prioritization of information systems across the State's IT enterprise. While OIT had worked, in conjunction with Business Owners, to identify critical and essential systems for each consolidated agency, the current number of critical and essential systems across all consolidated agencies is over 200. Additional analysis and coordination are needed to prioritize the list of critical and essential systems across all agencies, to enable OIT to focus its limited resources on those activities and initiatives that are most critical to the State's mission and priorities. A clear understanding of cross-agency priorities would serve to focus and improve all aspects of OIT's responsibilities and services. Fundamental security and operational activities such as planning and executing disaster recovery, responding to incidents, patching and updating systems, resolving helpdesk tickets, conducting risk assessments, and developing system security plans could all be approached by OIT with greater focus and assurance.

   OIT has not provided a formal explanation for why they have not established an effective and holistic approach for the prioritization of information systems across the State's IT enterprise.

   NIST 800-53 Section Contingency Plan | Identify Critical Assets, CP-2(8) states that organizations should identify critical system assets supporting mission and business functions. The *identification of critical information assets also facilitates the prioritization of organizational resources.*

NIST 800-53 Section Security Categorization | Impact-level Prioritization, RA-2(1) states that organizations should conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

NIST 800-53 Section Criticality Analysis, RA-9 states that organizations identify critical system components and functions by performing a criticality analysis for information systems at organization-defined decision points in the system development life cycle.

3. OIT had not effectively communicated the release of updated security policies to those who were responsible for their implementation and execution. Staff we interviewed at the sample of consolidated agencies indicated that the OIT's only notification to consolidated agencies of the updated March 2022 CISP updates was sent out via email on the day the CISPs were released and went into effect. When we talked to staff in September 2022, six months after these policies went into effect, four of five consolidated agencies interviewed were not aware of updates made to CISPs, which included significant changes to agency responsibilities. Below are some of the responses we received from various levels of agency management at the consolidated agencies, when we discussed the release of these updated CISPs:

   - When we asked consolidated agency staff about receiving an email from OIT announcing the new policies, they responded, "I remember receiving an email from OIT but there's been no follow up."

   - When we explained to consolidated agency staff that OIT has released new versions of the CISPs in March 2022, they responded, "We assume they would tell us what to do because that's the model that was established when OIT was created."

   - When we asked consolidated agency staff if anyone at their agency received training on their responsibilities outlined in these updated policies they responded, "I guarantee that didn't happen."

   The one agency that stated they were aware of the recent updates to the CISPs acknowledged that they were made aware of these updates through another OSA state audit. They further explained that, once they had reviewed the updated CISPs, their perspective was that "we don't know how to operate in this new world," and that they, "…chose to follow the old policies."

   In addition, six months after these policies had gone into effect, OIT had still not established an approach for communicating expectations to agencies or their contractors. In an interview with one IT director, they stated that "Vendors don't know that the policies have changed. It would have been up to the agency to inform their vendors."

   OIT has not provided a formal explanation for why the deployment of CISP updates was not properly communicated to all users, especially Business Owners and their vendors. In discussing shortcomings in the rollout of the March 2022 CISPs with representatives of the Governance and Cybersecurity Team within the OIS, who oversaw their development and communication, they explained that they, "…are not policy experts."

Section 24-37.5-401(1)(e), C.R.S., requires that information security policies must be implemented throughout public agencies, such as the 5 consolidated agencies selected for testing, to ensure the development and maintenance of minimum information security controls to protect communication and resources that support the operations and assets of those agencies.

Section 24-37.5-403(2)(b, c and d), C.R.S., states that the CISO shall promulgate rules pursuant to information security policies, standards, and guidelines; ensure the compliance with information security policies in the information security plans developed by public agencies; and direct information security audits and assessments in public agencies in order to ensure compliance and adjustments.

Standards for Internal Control in the Federal Government (Green Book) Principle 14.3, states that management should communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. In these communications, management should assign the internal control responsibilities for key roles.

4. OIT had not consistently defined who or what constitutes a Business Owner. OIT used the role of and term “Business Owner” haphazardly throughout many of its policies, procedures, and other formal documents. Further, OIT had not differentiated between enterprise-level, agency-level, and system-level ownership when referring to the Business Owner, leading to confusion on who is responsible or how a control is applied. Consider the following example:

The CISP for IT Security Planning (CISP-017) defines the Enterprise Cyber Security Plan (ESCP) as, “…an annual information security plan created by the Office of Information Security (OIS), within OIT, for the Consolidated Agencies. The plan includes an assessment of current risk, covers the incident response capabilities, disaster recovery capabilities, and a plan of action and milestones that describe current gaps in the security program and summarizes the goals of the OIT to address those gaps over the coming fiscal year.” This policy goes on to state that OIT, “…with input from the Business Owner, shall develop an enterprise cyber security plan (ECSP) for Business Owner [sic].”

In this instance, where an enterprise-wide plan is being developed, it is unclear who should be regarded as the Business Owner – an individual, an agency, or all consolidated agencies.

OIT has not provided a formal explanation for why there are inconsistencies in who or what constitutes a Business Owner.

Standards for Internal Control in the Federal Government (Green Book) Principle 3.06 states that, to achieve the entity’s objectives, management should assign responsibility and delegate authority to key roles throughout the entity.

Federal Information System Controls Audit Manual (FISCAM) Control SM-3.1 states that security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of information resource owners and users. Senior management and *information resource management have ultimate responsibility for providing direction and ensuring that information security responsibilities are clearly assigned and carried out as intended. Security plans should clearly establish who "owns" the various computer resources, particularly data files, and what the responsibilities of ownership are. If a resource has multiple owners, policies should clearly describe whether and how ownership responsibilities are to be shared.*

5. Business Owners (individuals) were not formally identified for a population of 384 applications managed by OIT, including 73 critical and essential systems. Where Business Owners (individuals) had been identified by OIT, our examination of system security plans, inspection of system inventories, and interviews with personnel at both OIT and consolidated agencies discovered inaccuracies and inconsistencies in who was acknowledged as the actual Business Owner. The table below provides several examples of these inaccuracies and inconsistencies.

System Name	Identification of Business Owner (Individual)
Example 1 **Application from the Colorado Department of Natural Resources (CDNR)**	Our discussions with agency staff and our review of the SSP identified two different Business Owners (individuals). In addition, the OIT system inventory did not identify a Business Owner (individual).
Example 2 **Application from the Colorado Department of Human Services (CDHS)**	Our review of the SSP and the OIT system inventory identified two different Business Owners (individuals).
Examples 3 and 4 **Applications from the Colorado Department of Labor & Employment (CDLE)**	Our discussions with OIT staff and our review of the SSP and OIT system inventory identified three different Business Owners (individuals).
	Our review of the SSP and OIT system inventory identified two different Business Owners (individuals).

OIT has not provided a formal explanation for why Business Owners (individuals) were not formally defined for some applications. OIT did explain that they are currently building the inventory of all software assets and implementing processes across the participating agencies, suggesting that this new asset inventory would help ensure consistency in defining system roles.

The CISP Glossary states that, "…the agency or entity that is the Data Steward is also the Business Owner. The Business Owner has the authority to authorize or deny access to the data, and is responsible for the accuracy, integrity, and timeliness of the data."

Federal Information System Controls Audit Manual (FISCAM) Control SM-3.1 states that security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of information resource owners and users. Senior management and *information resource management have ultimate responsibility for providing direction and ensuring that information security responsibilities are clearly assigned and carried out as intended. Security plans should clearly establish who "owns" the various computer resources, particularly data files, and what the responsibilities of ownership are. If a resource has multiple owners, policies should clearly describe whether and how ownership responsibilities are to be shared.*

6. For the fifteen systems we tested during this audit, OIT was unable to provide documentation of the security decisions that were made by the systems' respective Business Owners. The CISPs that were developed and released by OIT in March 2022 include 166 security decisions or responsibilities that were assigned to Business Owners – a significant increase over previous CISPs. These changes warranted an intentional communication and education plan by OIT to ensure information security policies had been implemented throughout consolidated agencies.

   OIT has not provided a formal explanation for why they could not provide documentation or evidence of the security decisions made by system Business Owners. However, it was noted that OIT had not established a process or approach for educating Business Owners on changes to their responsibilities and the security decisions Business Owners would need to make that resulted from the changes in the CISPs. The documented decisions are necessary for OIT to ensure that those decisions are referenced when implementing security controls as the IT service provider for the various Business Owners.

   Section 24-37.5-401(1)(e), C.R.S., states that information security policies must be implemented throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and resources that support the operations and assets of those agencies.

7. OIT had not established minimum security requirements for key security activities – for example, audit logging, session time outs, user account reviews, data backup frequency, and security training. While OIT has established a set of best practices or guidelines in the *CISP Supplemental Guidance*, these are not requirements and do not ensure a consistent, minimum level of security across the enterprise.

   OIT has not provided a formal explanation for why minimum-security requirements for key security activities have not been established. However, members of the CISO's Governance and Oversight team explained that their purpose in not establishing minimum security requirements is to allow individual business units to tailor security to their needs.

   OIT's Enterprise Cyber Security Plan, in outlining roles and responsibilities, states that OIS sets minimum security requirements for all public agencies.

   Section 24-37.5-401(e), C.R.S., states that information security standards, policies, and guidelines must be promulgated and implemented throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and information resources that support the operations and assets of those agencies.

8. Twenty-one of the twenty-eight (75 percent) Technical Standards published by OIT had not been reviewed in over five years, and only 1 of the 28 (4 percent) Technical Standards had been

reviewed in the past 12 months. While we noted this as a problem during our audit, we also recognize that OIT has a current IT Governance finding and recommendation from the OSA's Fiscal Year 2021 Statewide Financial and Compliance audit that is outstanding, with a December 2022 implementation date provided by OIT. We have nevertheless included this as an issue in our report because it impacts OIT's cyber resiliency when aggregated with the other problems we found.

OIT explained that the Technical Standards are individually owned and that efforts had been made in recent weeks to reach out to the respective Technical Standards' owners to conduct reviews of these standards, but without significant response.

Section 8 of each Technical Standard states that the standard is to be reviewed every six to twelve months by the document owner and remains in effect until otherwise noted.

Why do these problems matter?

Many of the problems identified relate to practices that form the foundation of an organization's IT security program, including the setting of standards and the defining of roles and responsibilities. Since perceptions and understanding of security vary, these activities provide guidelines and expectations to those responsible for implementing and managing security to ensure consistency throughout the enterprise. Without these aspects of governance and oversight, IT security may be erratically applied across organizations or systems.

Without clear and decisive direction of its role with consolidated agencies, OIT cannot provide effective IT services. Further, as a result, overall security is reduced as there is confusion on who is responsible for security-related controls and oversight when you have undocumented agreed-upon responsibilities shared across OIT, agencies, and third-party service providers.

Finally, without prioritization of information systems, OIT cannot ensure it effectively utilizes its time and resources across all its initiatives. Examples of this would be a large-scale outage where multiple critical and essential systems need to be restored. Without agreed-upon prioritization, all agencies will demand their information systems are most critical and expect services to be restored first. Another example would be a situation where an update or patch needs to be implemented immediately to all systems. Even relatively less-urgent, but no-less impactful activities, such as developing system security plans or conducting system risk assessments, will continue to be a struggle for OIT to accomplish without proper system prioritization.

Recommendation No. 1:

The Governor's Office of Information Technology (OIT) should improve governance and oversight controls by:

A. Complying with Colorado Revised Statutes by fulfilling the duties and responsibilities of the Chief Information Security Officer, as outlined in statute, including ensuring incorporation of and compliance with information security policies. If determined necessary, OIT should work with the General Assembly to more clearly define OIT's role as a provider of security services to consolidated agencies, and to clarify the intent of the General Assembly regarding OIT's role in the State's information technology framework.

B. Formalizing an approach and strategy to prioritize information systems across all consolidated agencies. This prioritization should be based upon the processes and services that are most critical to the State's mission and objectives. As such, coordination and involvement of leadership at the State and Agency levels should be a key component of this prioritization process. Once completed, OIT should utilize the list to prioritize activities and initiatives, such as conducting risk assessments, developing system security plans, and testing disaster recovery/ incident response plans.

C. Formalizing standard operating procedures for the release of new or updated security policies, including the communication and education of all impacted parties. These procedures should include proactive communications to notify users of upcoming changes, multiple forms of communications (including, but not limited to, emails, posts, presentations, and face-to-face), and posting of updated communications to ensure users retain information. In addition, OIT should consider an implementation period for when new or updated security policies are communicated and issued, prior to the effective date.

D. Setting, documenting, and communicating a clear and consistent definition for the role of Business Owner throughout the State's information security programs, policies, and plans. In addition, the definition should differentiate between enterprise-level, agency-level, and system-level ownership when referring to the roles and responsibilities of a Business Owner.

E. Implementing Recommendation Parts A and B within the confidential Asset Management finding, then working with agencies to identify Business Owners for all applications managed by OIT and ensuring these roles are consistently defined in system security plans and system inventories.

F. Formalizing a process or approach for defining the security requirements, decisions, and responsibilities of Business Owners, especially those outlined in the Colorado Information Security Policies released in March 2022. Once a process or approach is established, formalizing a training program for all Business Owners that outlines their roles and responsibilities.

G. Establishing minimum security requirements for key security activities, including but limited to, audit logging, session time outs, user account reviews, data backup frequency, and security training. These minimum-security requirements would act as a baseline, and Business Owners could adopt more stringent security requirements to meet management's expectations and risk tolerances.

H. Continuing its effort to review its Technical Standards and establishing a process to have these standards reviewed by appropriate personnel, at minimum, on an annual basis.

Agency Responses:

A. **Disagree**. **Implementation Date: N/A.**
The Governor's Office of Information Technology (OIT) disagrees with this finding. CISO continues to work off of existing interpretation of statute; 24-37.5-403 which states in part (4) The chief information officer may promulgate as rules pursuant to article 4 of this title 24, all of the policies, procedures, standards, specifications, guidelines, or criteria that are developed or approved pursuant to section 24-37.5-105 (4). CISO will reach out to General Assembly to more clearly define OIT's role as a provider of security services to consolidated agencies, and to clarify the intent of the General Assembly regarding OIT's role in the State's information technology framework.

AUDITOR'S ADDENDUM: Our recommendation does not dispute OIT's statutory authority and responsibility to promulgate (i.e., promote or make widely known) policies, procedures, standards, etc. Rather, as noted in the finding, statute further assigns responsibilities to OIT that align with an entity responsible for directing consolidated entities' overall IT posture, such as ensuring compliance with information security policies and establishing and directing an IT risk management process to identify security risks and deploy risk mitigation strategies. OIT's defining of its roles and responsibilities through its CISPs as those limited to a *service provider* role do not appear to align with its statutory responsibilities.

B. **Partially Agree. Implementation Date: March 2024**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. As mentioned below, there is an existing formal approach and strategy in place for prioritizing, hence the partial agreement. The ePMO gating process includes rating the overall system classification (Essential, Critical, Business Priority) in the Discovery phase of project gating. The Technology Planning Workbook (TPW) processes involves prioritizing information systems, which is a partnership with the agency business owners and technical offices of OIT. Also, we are transitioning from: Three Levels Critical, Essential and Business Priority to four tiers: Tier 1, Tier 2, Tier 3, Tier 4.
Essential + --> Tier 1
Essential --> Tier 2 (life and limb takes highest priority)
Critical --> Tier 3
Business Priority --> Tier 4
Currently, we don't have any Tier 1 systems noted yet, but they will have a recovery window of less than 4 hours. We'll officially ask agency business owners and technical offices of OIT for this criticality data to be refreshed next in the first quarter of 2024 to update the Configuration Management Database (CMDB), but agencies can update this any time in TPWs. Once the tiers are implemented in the CMDB, current processes will reflect the changes.

AUDITOR'S ADDENDUM: As noted in the finding, although OIT has a system classification process, its process does not adequately consider the priority of systems within each classification tier, such as by most to least critical, in order to provide essential direction for system recovery efforts when a major incident or disaster occurs, or when systems need security updates or security risk assessments. OIT's current process of organizing thousands of state systems into a handful of large groups only provides a small insight into which systems are more critical than others.

C. **Agree. Implementation Date: July 2023.**
The Governor's Office of Information Technology (OIT) agrees with this finding. With regards to communicating changes to users via email, we have added a "Do Not Delete" label for all customer notification emails. In the past, users would inform OIT that the change was not communicated. Since the email retention policy deleted emails, OIT had no way to refute the claim. With the Do Not Delete label, OIT can now go back to all sent notifications and confirm user(s) received the notification. When Office of Information Security (OIS) updates the policies, they will keep a copy of the Service Desk notice and who it will be sent to for future record. Security Governance will update it's internal SOP to reflect the change by 7/1/2023. OIT security governance is developing a security communications plan with OIT's communications team as well as the OIT Service Desk to ensure changes to policy or process that impact customers are communicated effectively and timely to ensure user awareness of the updates. This will include open office hours to answer questions with stakeholders, lunch learning sessions, tracking of communications sent out, and seeking feedback from our customers about the notices we send out. Updates to the process to improve this flow will be communicated internally with OIT staff as well to ensure awareness around the importance of tracking the communications sent out.

AUDITOR'S ADDENDUM: The response provided by OIT does not adequately address all aspects of our recommendation. Specifically, as OIT enacts policies related to the communication of new or updated security policies, OIT should consider an approach to ensure an appropriate implementation period is provided prior to the policy effective date.

D. **Agree. Implementation Date: July 2024.**
The Governor's Office of Information Technology (OIT) agrees with this finding. Project is currently underway, however no time line currently exists for completion. The system identification component is not completed yet and a completion date has not been identified yet. OIT security is working with it's partners to review and provide better clarity around roles and responsibilities as well as better defining those roles. Often times, a business owner might be an agency, or a program, or line of business within a program. This leads to confusion. OIT will accomplish this not later than July 1st 2024. In the ensuing time OIT is working to provide more clarity and guidance for each role in the service delivery model. Your example about the ECSP is correct, it's not clear. Business owner in the case of the ECSP means each agency and should say that. Additionally, OIT is revamping it's ECSP/ACSP process and requirements based on some of the audit finding contained herein.

E. **Agree. Implementation Date: May 2024.**
The Governor's Office of Information Technology (OIT) agrees with this finding. Project is currently underway, however no time line currently exists for completion. The system identification component is not completed yet and a completion date has not been identified yet. Once the software asset management system is up and running, along with the application portfolio management module, they will work together to identify service and asset owners. The software asset management module is set to be 100% functional around January 2024. The application portfolio management module has yet to be launched, which is why this item cannot be completed just yet.

F. **Partially Agree. Implementation Date: June 2024**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. The disagree is that OIT does work with agencies to document how security controls are implemented. This is first introduced in the Project Life Cycle and then in the work we do with the agency in the development of their System Security Plans. We agree that OIT needs to work on the automation of the work flow, auto selection of architectural reference models, selection of logging requirements based on the system data classification. These are all components being created and adopted in ServiceNow. This is a multi-phased project that will occur over the next few years.

AUDITOR'S ADDENDUM: As discussed in the finding, for a majority of systems we tested, OIT could not provide an updated, current SSP or provide evidence that conversations with Business Owners on security related controls had taken place. By not working with Business Owners to document their security requirements, OIT is unable to ensure that they are compliant with CISPs. If systems do not comply with security requirements, there is an increased risk of a cyber incident.

G. **Partially Agree. Implementation Date: June 2024**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. We fundamentally disagree that we don't establish a security baseline. CISPs cover baselines for backups, session timeouts, reviews. These are the minimums. How that baseline is implemented/established is up to the organization that the policy applies to. We specifically state in security policy that the agency may and will most likely have additional security requirements beyond the CISP's baseline security requirements. As an example, security screen lock timeout - this is required in policy. What's not in policy is what the minimum length of that timeout is. That is a SHARED decision between OIT and the agency to decide based on their unique business requirements, regulatory requirements, and risk tolerance with input from OIT security SME's. System health and performance issues are all baselined and reportable via application and system logging. However, from OIS's Security Governance perspective, OIT lacks a comprehensive logging strategy. Governance will work with internal teams and stakeholders to draft a logging standard and put it forward for approval and adoption. Governance will have a draft of the logging standard by OCT 2023. IT Ops teams to implement logging standard by end of FY24. All other components listed in the finding are actively being done as part of day to day administration practices and documented for the enterprise in the form of a document data backup strategy, COOP, security training for users. Logging is addressed in this response because the auditor used logging as an example. We responded to your example by illustrating our approach on the topic.

AUDITOR'S ADDENDUM: We acknowledge and agree that the CISPs establish the existence of security requirements. However, they do not establish the minimum requirements that would constitute a security baseline. By OIT simply providing departments with general security requirements with no minimum standard or expectation, there is a risk that the departments involved in defining security activities for a system may adopt a standard that does not conform to industry best practices or exposes the State to unnecessary risk. This problem is further exacerbated because OIT does not currently have a formal process to document Business Owners requirements (see Part F of the recommendation above). Since OIT has the expertise in and responsibility for cybersecurity, it is in the State's best interest for OIT to define and enforce minimum security standards.

H. **Agree. Implementation Date: September 2023.**
The Governor's Office of Information Technology (OIT) agrees with this finding. Once we deploy PSDS (Public Service Digital Service) module in ServiceHub, we will have the ability to set annual reminders and also share the standards to external customers. Current time line is September of 2023 as we just procured this ServiceHub module and will need to work with Communications and Technical Standards owners on the new process.

Finding 2: Information Security Training and Awareness

The Governor's Office of Information Technology (OIT) develops and documents information security training and awareness materials for OIT personnel and staff at the consolidated agencies. As part of the security training, OIT creates an Acceptable Use Policy that all users have to read and sign their acknowledgement of annually. The Office of Information Security (OIS), within OIT, is responsible for ensuring all OIT personnel complete information security training on an annual basis. In addition, OIS periodically distributes training materials to consolidated agencies, but agencies are responsible for ensuring the security training is completed by all personnel. Agencies are required to provide training completion reports to OIT on a quarterly basis.

Colorado Information Security Policy (CISP) requires security awareness training to be conducted with each new user within OIT and consolidated agencies as part of the onboarding process. All users are then required to participate in security awareness refresher training annually. The annual training developed by OIS is divided into modules that are distributed to users throughout the year on a quarterly basis.

What audit work was performed and what was the purpose?

To conduct our audit and support our conclusions, we conducted interviews with OIT management and staff and a selection of staff from a sample of five consolidated agencies to understand the policies and practices in place for providing security training and awareness. Specifically, we:

- Discussed training requirements for general users, as well as additional role-based training provided to applicable OIT and agency staff.
- Reviewed security training and awareness materials developed and distributed by OIS.
- Tested training records for a sample of agency and OIT personnel to determine compliance with applicable CISPs.

The purpose for the audit work performed was to evaluate OIT's design and implementation of control activities related to information security training and awareness, and the impact on OIT's cyber resiliency.

What problems did the audit work identify, how were the results measured, and why did they occur?

We identified problems with OIT's information security training and awareness controls, as noted below, along with the reasons the problems occurred:

1. OIT has not provided role-based security training to personnel who are responsible for information security activities. Our testing specifically identified the following:

   - OIT has not ensured Business Owners received training in their security roles and responsibilities. Leadership we interviewed at a selection of five consolidated agencies all confirmed that their personnel never, at any point in time, received training or instruction on their security roles and responsibilities as Business Owners.

   - OIT has not ensured IT directors received training on their security roles and responsibilities. In conversations with a selection of five IT directors, all five indicated that they were not provided guidance or instruction on their responsibilities for key security activities, including, but not limited to, the maintenance of System Security Plans (SSP), the handling of quarterly agency security report cards, or the implementation of the Colorado Information Security Policies (CISPs). In speaking with one IT director about expectations or training of IT directors, they stated, "there is no playbook," and that their responsibilities "…change from week to week."

   OIT has stated that IT directors had not received role-based security training due to a lack of OIT resources with personnel to provide one-on-one training for IT directors.

   Standards for Internal Control in the Federal Government (Green Book) Principle 4.05 states that management should enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.

   Federal Information System Controls Audit Manual (FISCAM) Control SM-3.1 states that management should ensure that employees—including data owners, system users, data processing personnel, and security management personnel—have the expertise to carry out their information security responsibilities.

   C.R.S., 24-37.5-403(2)(g) states that the CISO shall conduct information security awareness and training programs.

   CISP-002 Section 9.2.1 states that OIT shall provide role-based security awareness training to IT personnel according to their IT responsibilities on a regularly scheduled basis.

2. OIT had not ensured all users completed security awareness training on a regular basis. Our testing identified the following:

- 4 of 24 (17 percent) employees we tested across five consolidated agencies and OIT had not completed quarterly security training in a timely manner. Specifically, the four employees had not completed at least one of the quarterly trainings from the last four quarters.

- 14 of 18 (78 percent) external users we tested across five agencies and OIT had not completed quarterly security training in a timely manner. This testing included three OIT contractors, of which two had not completed any type of security awareness training.

OIT has not provided an explanation for why OIT users had not completed quarterly security training in a timely manner. OIT has stated it is not their responsibility to ensure users at consolidated agencies receive training, but only to provide training materials. However, Colorado statute states that the CISO shall conduct information security awareness and training programs. Conducting an information security awareness and training program consists of more than simply providing training materials. As described in the NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* an information security awareness and training program also consists of the following:

- Developing an awareness and training plan
- Communicating the plan
- Monitoring compliance
- Collecting and evaluation and feedback
- Ongoing improvement of the program

C.R.S., 24-37.5-403(2)(g) states that the CISO shall conduct information security awareness and training programs.

NIST CSF Practice AT-1 states that all users should be informed and trained on their security responsibilities.

NIST 800-53 Control AT-2a states that organizations should provide security and privacy literacy training to system users (including managers, senior executives, and contractors).

NIST SP 800-50, Building An Information Technology Security Awareness and Training Program, provides guidance for building an effective information technology security program, including details for program design, material development, program implementation, and post-implementation.

OIT Enterprise Security Plan (Page 26) states that all employees receive training within 30-days of onboarding and then are required to complete quarterly refresher security awareness training or face possible corrective action. Additionally, access to this same training content is made available to all contract employees with access to state systems or data.

3. OIT had not ensured the Acceptable Use Policy (AUP) was signed by all users on an annual basis. Our testing identified the following:

- 2 of 24 (8 percent) users we tested across five consolidated agencies and OIT had not completed a signed acknowledgement of the AUP in the past twelve months.

- 14 of 18 (78 percent) contractors we tested across five consolidated agencies and OIT had not completed a signed acknowledgement of the AUP in the past twelve months.

OIT has not provided a formal explanation for why OIT users had not reviewed and acknowledged the AUP on an annual basis. However, OIT has stated that their responsibility is not to ensure users at consolidated agencies acknowledge the AUP, but only to make the AUP available.

CISP-018 Acceptable Use of State Data and IT Resources (AUP) Section 17[2] states *that this policy must be accepted by users at the start of employment and no less than annually thereafter. The CISPs define "users" as, "All State of Colorado employees, temporary workers, contractors, interns, volunteers, third-party vendors and any others who have been granted access to non-public state IT resources."*

Standards for Internal Control in the Federal Government (Green Book) Principle 5.03 states that management should hold entity personnel accountable for performing their assigned internal control responsibilities.

Standards for Internal Control in the Federal Government (Green Book) Principle 5.05 states that management should hold service organizations accountable for their assigned internal control responsibilities.

Why do these problems matter?

Educating users on their cybersecurity responsibilities is critical to ensuring the reliability and protection of state information systems and data. Role-based security training for all personnel who conduct security-related functions is also an essential activity for successfully implementing critical security controls. Without this training, staff may not be aware of the current security requirements and therefore, may not implement the requirements. Without effective training and awareness on current social engineering threats and attacks (i.e., phishes, ransomware attacks, etc.), users may also not be aware of these threats and how to handle them to mitigate or prevent them from exploiting IT environments, systems, or data.

Recommendation No. 2:

The Governor's Office of Information Technology (OIT) should improve information security training and awareness by:

A. Establishing a formal training program for Business Owners that outlines and provides necessary direction on their security roles and responsibilities, especially those outlined in the Colorado Information Security Policies (CISPs).

[2] CISP-018 *Acceptance Use of State Data and IT Resource (AUP)* was updated by OIT in December 2022 – after our fieldwork was completed. With this update, the section referenced was changed from Section 17 to Section 18.

B. Utilizing resources in more efficient ways to ensure IT directors receive formal training on their security roles and responsibilities, especially those outlined in the CISPs.

C. Enforcing sanctions for users who do not complete security awareness training in a timely manner.

D. Enforcing sanctions for users who do not review and acknowledge the State's Acceptable Use Policy at the start of employment and annually thereafter.

Agency Responses:

Recommendation No. 2:

A. **Partially Agree. Implementation Date: June 2025**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. This is an area in which we are actively looking to establish specific role based training options for our IT Directors, agencies and customers. OIT is working with a vendor on identifying potential solutions. We disagree that they do not receive training on their responsibilities. We agree that the specific role based training is lacking and we are working on those options. We disagree that OIT has shifted the majority of security related decision to the business owners. In fact we assert that we have done the opposite. We're including them in the decision making process rather than dictating a proscriptive set of requirements. We agree that Roles and Responsibilities can be more clearly defined to reduce confusion and enhance clarity on who owns what. OIT's changes to policy were an attempt to address the incorrect perception that it's up to OIT security to define agency business requirements. It's a partnership, not a transfer of ownership. OIT continues to work with business owners to see what additional training may be needed. OIS, business owners and IT Directors plan and hold table top exercises for critical and essential systems at least twice a year. Their role in the incident response process is exercised and explained during these exercises. OIT does provide online cyber security awareness training to all staff that advises them of their responsibility to ensure the protection of data, report suspected breaches, and advises them of appropriate behavior when using state IT systems. OIT will continue to review it's training opportunities and look for training content that is closer in line to "Role Based" and implement over the coming two fiscal year cycles.

AUDITOR'S ADDENDUM: As noted in the finding, OIT has not provided specific role-based training to personnel responsible for IT security activities, which IT acknowledges in its response. Furthermore, OIT's statement that they have included Business Owners in the decision-making process further supports the need for establishing training for Business Owners on their security-specific responsibilities – above and beyond the general cyber security awareness training provided to all staff.

B. **Partially Agree. Implementation Date: June 2025**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. The portion that we are disagreeing with is that IT Directors don't receive any role based training as it relates to cyber security as evidenced by that fact that each IT Director must take all OIT assigned learning. This includes mandatory cyber security awareness training, which includes data classification and handling, CISP overview training, Security and Privacy Training, OIT IT

Compliance Audit and Audit procedure training along with monthly security updates from OIT's monthly newsletter, All Manager's meetings, and others. What we do agree with is Role Based Training can and should be improved so that all roles within OIT understand their responsibilities around cyber security.

OIT does provide security awareness training. OIT tracks and maintains the training history of all employees including IT Directors and agency employees that use OIT's LMS. The agencies that have their own LMS use our training content and provide to their users and report of OIT on their user's progress. The CISPs do include what the roles are for ITSP and Business Owners. Last training cycle OIT and it's agency partners reached a total completion rate of 93% across all OIT supported agencies including itself. The agencies are responsible for verifying the compliance with their users / contractors completing the training. OIT HR works with employee's supervisor when training is not completed in a timely manners. OIT will continue to review it's training opportunities and look for training content that is closer in line to "Role Based" and implement over the coming two fiscal year cycles.

AUDITOR'S ADDENDUM: OIT's response does not address the recommendation for role-based training specific to the security responsibilities of IT directors. CISP-002, Section 9.2.1 requires OIT to provide role-based training to IT personnel. During our audit, OIT stated that they did not have the resources to provide role-based training to IT directors on their responsibilities, and we spoke with the IT directors at five agencies or offices supported by OIT, and all five indicated they were not provided guidance or instruction on their responsibilities for key security activities. If OIT does not provide role-based training to IT directors, there is an increased risk of system misconfigurations or confusion on the implementation of specific security controls.

C. **Partially Agree. Implementation Date: December 2023**.
The Governor's Office of Information Technology (OIT) partially agrees with this finding. OIT published in 2021 the "Required Training Graduated Sanctions Policy", which is also posted on OIT Plaza for OIT employees. OIT HR has not had a need to apply this policy to OIT employees. However, CISP-002 as well as CISP-018 does provide sanction up to and including suspension within compliance section that includes loss or reduced access, suspension to state IT resources. OIT agrees that additional efforts and focus need to be applied to monitoring and enforcing existing policies in effect, strengthening focus in tracking and updating and maintaining those records.

AUDITOR'S ADDENDUM: It is a best practice for all users to complete security awareness training on a regular basis. While OIT's response only addresses OIT users, our testing identified both OIT and agency users who did not complete security awareness training in a timely manner, yet OIT indicated that it has not applied sanctions for any noncompliance. Further, although OIT has stated that it has developed a sanctions policy, this policy only applies to OIT staff – not to those users outside of OIT. Therefore, those users outside of OIT may not be aware of the possibility of sanctions for not completing the required security awareness training in a timely manner. If all users are not provided security awareness training, it leaves the organization vulnerable to potential cyber threats.

D. **Partially Agree. Implementation Date: December 2023**.

The Governor's Office of Information Technology (OIT) partially agrees with this finding. OIT published in 2021 the "Required Training Graduated Sanctions Policy", which is also posted on OIT Plaza for OIT employees. OIT HR has not had a need to apply this policy to OIT employees. However, CISP-002 as well as our CISP-018 does provide sanction up to and including suspension within compliance section that includes loss or reduced access, suspension to state IT resources. OIT agrees that additional efforts and focus need to be applied to monitoring and enforcing existing policies in effect, strengthening focus in tracking and updating and maintaining those records.

AUDITOR’S ADDENDUM: The March 2022 CISP-018 Section 17 requires all users to review and acknowledge an Acceptable Use Policy (AUP) and provides actions that will be taken if users fail to comply with the policy, including the annual acceptance of the AUP. While OIT’s response only addresses OIT users, our testing identified both OIT and agency users who did not complete an annual AUP in a timely manner, yet OIT indicated that it has not applied sanctions for any noncompliance. Failing to ensure that all users acknowledge an AUP and not assessing sanctions for noncompliance leaves the State vulnerable to cyber threats and lawsuits.

Glossary

The list of terms below are partially based on Colorado Information Security Policies and Technical Standards.

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Consolidated Agency

Refers to those state agencies whose IT functions were consolidated under OIT pursuant to Senate Bill 08-155 and defined in C.R.S.24-37.5-102(28). This includes most executive branch departments except for institutions of higher education.

Critical System

A system that provides crucial services to the public and its operation serves a vital function to state government. This includes systems that process benefits, payments, revenue and similar transactions, and include direct use by residents and service providers (e.g., Medicaid payment systems, online driver license renewals, reservation systems such as parks, etc.). Critical applications also service multiple divisions or programs within a single agency or across multiple agencies.

Cyber Resiliency

An entity's ability to continuously deliver the intended outcome, despite cyber-attacks.

Data Center

A building, a dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Data Steward

The Agency/Business Owner.

Essential System

A system that is so important to the agency that its loss or unavailability is unacceptable due to life-safety issues. These are systems that have direct contact with Coloradans and service providers and include systems that maintain human life, health or safety, and/or support emergency response.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Technology Service Provider (ITSP)

A service provider is a vendor or agency that provides IT solutions and/or services to end users and organizations.

IT Asset

A piece of software or hardware within an information technology environment.

IT Infrastructure

The composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment.

National Institute of Standards and Technology (NIST)

NIST is located within the Federal Department of Commerce and develops standards that are applicable to the federal government and can be adopted by other organizations.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Non-Consolidated Agencies

Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the "Organizations Affected" section of this policy.

Public Agency

Include both consolidated and non-consolidated agencies, except institutes of higher education and the General Assembly.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Software

A set of instructions, data, or programs utilized to operate a computer and execute specific tasks.

System

For the purpose of this audit, the OSA defines a "system" as an application, the application's operating system(s), and the application's database(s).

System Security Plan

Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Vulnerability

Flaws in a computer system that weaken the overall security of the device/system.