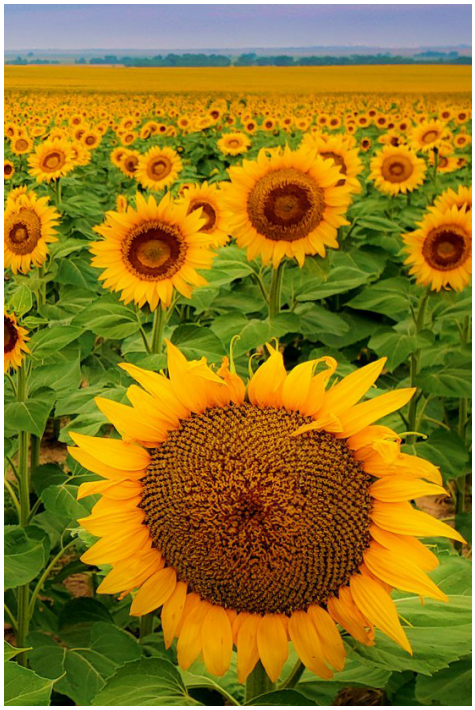
COLORADO OFFICE OF THE STATE AUDITOR | OSA

Governor's Office of Information Technology

Cybersecurity Resiliency

IT Performance Audit
January 2026
2551P-IT
Public Report





Legislative Audit Committee

Senator Lisa Frizell Chair	**Senator Dafna Michaelson Jenet** Vice Chair
Representative Jennifer Bacon	**Senator Rod Pelton**
Representative Max Brooks	**Senator Mike Weissman**
Representative Dusty Johnson	**Representative Jenny Willford**

Office of the State Auditor

State Auditor	**Kerri L. Hunter, CPA, CFE**
Chief IT Auditor	**Matt Devlin, CISA, CISM**
Audit Manager	**Cindi Radke, CISA**

OFFICE OF THE STATE AUDITOR

C O L O R A D O

Working to improve government for the people of Colorado.

OFFICE OF THE STATE AUDITOR

KERRI L. HUNTER, CPA, CFE • STATE AUDITOR

January 21, 2026

Members of the Legislative Audit Committee:

This report contains the results of an IT performance audit of Cybersecurity Resiliency at the Governor's Office of Information Technology (OIT). The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of OIT.

Government Auditing Standards allow for information that is considered sensitive in nature, such as detailed information related to information technology system security, to be issued through a separate "classified or limited use report," because of the potential damage that could be caused by the misuse of this information. We consider the specific technical details of Findings 3-12 and the related recommendations, to be sensitive in nature and not appropriate for public disclosure. Therefore, we have provided the details of these findings and recommendations to OIT management and to the Legislative Audit Committee in a separate, confidential report.

Kerri L. Hunter

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

Contents

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

Report Highlights

Cybersecurity Resiliency

Governor's Office of Information Technology

IT Performance Audit • January 2026 • 2551P-IT

OFFICE OF THE STATE AUDITOR
COLORADO

Key Concerns

The Governor's Office of Information Technology (OIT), as of June 30, 2025, had not fully implemented our May 2023 Audit of Cybersecurity Resiliency at OIT (Public Report) recommendations in the areas of IT Governance and Information Security Training and Awareness.

Additionally, OIT did not fully implement our May 2023 confidential audit report recommendations in the IT areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access, Risk Management, Security Planning, User Access Management, and Vulnerability and Patch Management.

Of the 71 prior recommendations that we performed follow-up testwork on as part of this audit, we determined that OIT had:

- **Implemented** 10 recommendations (14 percent)
- **Partially Implemented** 53 recommendations (75 percent)
- **Not Implemented** 8 recommendations (11 percent)

Without fully addressing our prior cybersecurity resiliency recommendations, OIT may not be able to fully meet its statutory responsibilities to ensure that information that Colorado's citizens have entrusted to state agencies is safe, secure and protected from unauthorized access, unauthorized use, or destruction [Section 24-37.5-401(b), C.R.S.].

Key Findings

- **IT Governance:** OIT did not provide sufficient documentation to demonstrate that it coordinated with state agency staff on its new process for system classifications that are based on how important the system's availability is to the agency's mission. In addition, OIT did not respond to inquiries made during the audit to clarify whether it was attempting to transfer its statutory authority to the various state agencies for ensuring their compliance with security policies and conducting information security audits and assessments. Specifically, OIT's December 2024 Colorado Information Security Policies (CISP) required various state agencies to be "responsible for contracting for security and compliance and that there is a validation of compliance." Additionally, OIT did not provide sufficient documentation that its Technical Standards had been updated and approved by OIT management and that the Technical Standards consistently established minimum security requirements.

- **Information Security Training and Awareness:** OIT indicated that it does not plan to provide training to state agency staff on their security responsibilities, even though it agreed to do so at the time of the May 2023 audit, and even though OIT's December 2024 CISPs assign security responsibilities to agency staff. Further, OIT indicates that it does not plan to provide training to its IT Director staff who support agency staff in conducting their IT-related responsibilities, even though OIT has also assigned them security responsibilities on which the IT Directors should be trained. OIT also failed to provide sufficient documentation that it assessed sanctions on its staff, as required by OIT's Business Operating Procedure for Noncompliance with Required Training, for their noncompliance with training and Acceptable Use Policy requirements.

Due to the sensitive nature of additional findings we identified through our follow-up audit—Findings 3 through 12—those detailed findings have been included in a separate, confidential report and provided to OIT.

Background

- OIT is the State's centralized IT department responsible for managing IT service delivery and resources, including personnel and equipment, for state agencies that have been consolidated under statute [Section 24-37.5-105, C.R.S.], as of July 1, 2008.
- The Chief Information Officer (CIO) is the state executive who leads OIT and is ultimately responsible for the security of state systems and information [Section 24-37.5-106, C.R.S.].
- The Chief Information Security Officer (CISO) reports to the CIO and serves as the point of contact for all information security matters in the State of Colorado. The CISO is responsible for informing the CIO and executive agency leadership of security risks and the impacts of policy and management decisions on IT-related initiatives [Section 24-37.5-403, C.R.S.].
- State agencies, also referred to as "consolidated agencies," are all of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government except for the following, which are referred to as "non-consolidated" agencies—Legislative Branch agencies; Judicial Branch agencies; the Departments of Education, Law, State, and Treasury; and state-supported institutions of higher education.

Audit Recommendations Made	Agency Responses		
	Agree	Partially Agree	Disagree
85	18	30	37

Chapter 1
Overview

Information security, as defined by the federal National Institute of Standards and Technology (NIST), is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." More specifically, cybersecurity focuses on the IT systems, or devices, securing data and information, including hardware and software. Similarly, cybersecurity resiliency, as defined by NIST, is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." An organization's cybersecurity resiliency is intended to enable its business and IT objectives to be met, even when information systems and resources are threatened by cybersecurity risks. NIST also provides industry leading frameworks of information security controls and resources to help organizations mitigate information and cybersecurity risks through their application and implementation.

Organizations can benefit from cybersecurity resiliency audits, as these types of audits can provide valuable insight to management, by evaluating the effectiveness of their cybersecurity processes, controls, and system environments. In addition, cybersecurity resiliency audits can aid organizations in identifying potential security gaps, including those related to whether they are in compliance with their own information security policies and procedures and applicable laws, regulations, and industry standards. Ultimately, cybersecurity resiliency audits can help organizations enhance their overall security postures and improve their abilities to identify, prevent, detect, respond to, and recover from cybersecurity incidents. In turn, organizations can increase their confidence level to ensure that they are properly managing and mitigating the risks associated with cyber threats, while at the same time minimizing potential impacts of system and data security breaches, which also helps to protect organizational reputations.

In 2023, we contracted with a CPA firm to conduct an IT performance audit titled Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology (May 2023 audit) to evaluate OIT's cybersecurity governance, risk management, and cybersecurity practices, including OIT's ability to identify, protect, detect, respond to, and recover from cybersecurity events and to determine its compliance with state policies, relevant laws, regulations, and leading industry standards. The audit also included a review of OIT's incident response plan, business continuity plan, and disaster recovery plan to determine whether they were up-to-date and effective. The May 2023 audit resulted in 77 public and confidential recommendations made to OIT, which were presented to the Legislative Audit Committee (LAC) in June 2023 through two separate public and confidential audit reports due to the sensitive nature of most of the findings. The overall findings identified in our May 2023 public audit report related to OIT's Governance and Oversight as well as Information Security Training and Awareness, and included the following issues:

- OIT had not clearly defined statewide security roles and responsibilities to align with those same responsibilities outlined in Colorado Revised Statutes. This ambiguity led to inconsistencies in the implementation of security practices and confusion on who was responsible for execution of security control activities—whether OIT, the various agencies that OIT supports, or third-party vendor.

- OIT had not established an effective and holistic approach for the prioritization of information systems across the State's IT enterprise.

- OIT had recently updated its Colorado Information Security Policies (CISPs) without proper education and planning to all affected parties. This lack of education exacerbated the security roles and responsibilities issues identified through the audit, as these updated policies migrated significant responsibilities from OIT to the agencies OIT supports.

- OIT had not established minimum security requirements for key security activities.

The audit identified additional findings 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.

In 2024, we conducted follow-up procedures to determine OIT's implementation status of the May 2023 audit recommendations. As of July 2024, OIT reported that 71 of the 77 of the May 2023 audit recommendations had not been fully implemented, and the corresponding audit status report was presented to the LAC in December 2024. In April 2025, during this audit, OIT's Chief Information Officer (CIO) stated that they planned to implement all of the remaining 71 recommendations by June 30, 2025.

Governor's Office of Information Technology

OIT is the State's centralized IT department responsible for managing IT service delivery and resources, including personnel and equipment, for state agencies that have been consolidated under statute [Section 24-37.5-105, C.R.S.], as of July 1, 2008. State agencies, also referred to as "consolidated agencies," are all of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government except for the following, which are referred to as "non-consolidated" agencies—Legislative Branch agencies; Judicial Branch agencies; the Departments of Education, Law, State, and Treasury; and state-supported institutions of higher education.

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
- IT economic development

OIT Leadership

The CIO is the state executive who leads OIT and is ultimately responsible for the security of state systems and information [Section 24-37.5-106, C.R.S.].

The Chief Information Security Officer (CISO) reports to the CIO and serves as the point of contact for all information security matters in the State of Colorado. The CISO is responsible for informing the CIO and executive agency leadership of security risks and the impacts of policy and management decisions on IT-related initiatives [Section 24-37.5-403, C.R.S.]. Specifically, the CISO's statutory responsibilities related to information security policies, standards, and guidelines include the following:

- Developing and updating information security policies, standards, and guidelines for "public agencies."
- Promulgating information security policies, standards, and guidelines.
- Ensuring the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by "public agencies."
- Directing information security audits and assessments in "public agencies" to ensure program compliance and adjustments.

Section 24-37.5-102(26), C.R.S. defines a "public agency" as, "…every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." As such, the statutory definition of "public agency" includes the consolidated agencies, or state agencies, as defined by statute, as well as the non-consolidated agencies of the Departments of Education, Law, State, and Treasury, as well as Judicial Branch agencies, but does not include the institutions of higher education or the Legislative Branch agencies.

Information Security Office

In performing the duties, the State CISO leads OIT's Information Security Office (ISO), which includes offices for Security Operations, Security Architecture, and Security Risk & Compliance. The

ISO is responsible for developing and maintaining state security policies—including CISPs—and providing leadership for state security initiatives. In addition, the ISO is also responsible for monitoring and tracking OIT's progress toward remediating audit recommendations.

Information Security Policies, Standards, Procedures, and Guidelines

The development and maintenance of IT policies, standards, procedures, and guidelines is critical for any organization, including OIT, to ensure that business and IT objectives are being achieved, and that the organization is able to respond to risks and meet management's expectations. As is the case with other large and complex organizations, OIT's policies, standards, procedures, and guidelines are far-reaching and apply across the entire organization, as well as to other state entities and vendors. OIT's policies, standards, procedures, and guidelines include the following:

- **Colorado Information Security Policies (CISPs).** According to Section 24-37.5-403, C.R.S., the CISPs are created by the CISO and issued by the ISO and are required to be implemented by OIT, public agencies, and vendors. The CISPs have historically been developed to align with certain industry leading standards, including NIST's Cybersecurity Framework (CSF) and Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, and the Center for Internet Security's (CIS) Critical Security Controls. This is consistent with how other states, such as Virginia and Arizona, for example, have documented their information security policies to align with NIST and other industry leading standards. The CISPs are intended to provide the CISO's high-level expectations related to required safeguards to secure state data and IT systems. At the beginning of this audit, OIT stated that it had early implemented the revised CISPs that it had updated as of December 2024, despite them all having "enforceable dates" as of July 1, 2025. During our May 2023 audit, we assessed OIT's implementation of the prior version of the CISPs, dated March 2022, as OIT had stated that it was operating under those CISPs at that time.

- **OIT Technical Standards.** The Technical Standards serve as more detailed specifications for the implementation of the CISPs, and they also apply to OIT, public agencies, and vendors. OIT has defined its Technical Standards as detailed specifications that contain measurable, mandatory requirements, or directives, to be applied to an information technology process, system, or action in order to carry out the CISPs and measure compliance with them. Further, during this audit, OIT stated that its established Technical Standards would act as a baseline and define minimum security requirements, instead of these minimum security requirements being included in the CISPs, as they had been prior to the CISPs dated March 2022. OIT's Technical Standards are developed and maintained by staff within OIT's various offices and divisions, such as those standards issued through the ISO under the CISO, or the Identity and Access Management division under the Chief Technology Officer (CTO), and are overseen by OIT's Office of Enterprise Architecture and approved by its Architecture Review Board (ARB). OIT's ARB is statutorily mandated (C.R.S. 24-37.5-105(4)) to advise the CTO and CIO on issues pertaining to IT standards. The ARB consists of five IT-related architectural domains: Business & Process

(BUS), Applications & Development (APP), Data (DAT), Infrastructure & Cloud Hardware/Software (INF), and InfoSec & Compliance (CISO).

- **Procedures and Guidelines.** OIT's procedures and guidelines, including its standard operating procedures (SOPs) and standard operating guidelines (SOGs), are also developed and maintained by staff within OIT's various offices and divisions. They are intended to provide the granular details of **how** the CISPs and Technical Standards are to be implemented to effectively manage security processes and maintain operational integrity. OIT has indicated that its procedures define OIT-wide technical or business processes, and they define the consistent and repetitive processes that OIT, agencies, and vendors should follow in order to comply with CISPs and Technical Standards. SOPs and SOGs fall within OIT's procedures category, but are much more specific, as they provide the step-by-step instructions on how to accomplish tasks so they can be completed consistently and correctly across the organization.

OIT stores and maintains its policies, standards, procedures and guidelines, collectively referred to as its "knowledge base," in its ServiceHub system. OIT's implementation of its ServiceHub knowledge base module is essentially an electronic library and serves as a single, centralized source of current documentation, accessible to both OIT and the public agencies, to help them gain efficiencies with information and knowledge transfer as it relates to OIT's policies, standards, procedures and guidelines. OIT went live with its ServiceHub system—specifically its customer portal—for OIT staff, contractors, and public agencies by Fall 2023.

Audit Purpose, Scope, and Methodology

We conducted this IT 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 April 2025 through December 2025. We appreciate the cooperation and assistance provided by OIT's management and staff during this audit.

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 objective of our audit was to assess whether the audit recommendations issued to OIT through the May 2023 audit were implemented to address the risks identified in the audit. This audit included considerations of OIT's updated management responses and action plans provided by OIT through its July 2024 Status Report for the May 2023 audit.

To accomplish our audit objective, we obtained and reviewed supporting documentation provided by OIT for the parts of the recommendations that OIT had indicated were either "implemented" or "partially implemented" by June 2025.

To support our audit conclusions, we measured OIT's implementation status against Colorado statutes or other state requirements; OIT's current adopted policies, procedures, standards, and/or guidelines; and other industry leading practices or standards. The industry leading practices or standards that we referenced during this audit included the following:

- U**.S. Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government (Green Book).**

  The Green Book prescribes internal control standards and provides criteria for an effective system of internal control for federal entities. In Colorado, the Colorado Office of the State Controller's policy, "Internal Control System," establishes that the State Controller has also adopted the Green Book as the State standard for internal controls and that state agencies, including OIT, must follow it for their system of internal control.

- **NIST Special Publications (SP), Frameworks, and Standards.**

  NIST, which is part of the U.S. Department of Commerce, provides industry leading frameworks of information security controls and resources to help organizations mitigate information and cybersecurity risks through their application and implementation. Specific NIST SPs, Frameworks, and Standards cited in our audit work included the following:

  - **SP 800-18**, Guide for Developing Security Plans for Federal Systems.
    Outlines the adoption of a minimum set of security controls, through the development of system security plans, that can protect an organization's information and information systems.

  - **SP 800-37**, Risk Management Framework for Information Systems and Organizations.
    Provides a repeatable process designed to promote the protection or information and information systems commensurate with risk.

  - **SP 800-50**, Building A Cybersecurity and Privacy Learning Program.
    Provides guidance for the development and management of an organizational life cycle approach to building a cybersecurity and privacy learning program that aims at encouraging behavior change, as part of risk management, and lead to developing a privacy and security culture.

  - **SP 800-53**, Security and Privacy Controls for Information Systems and Organizations.
    Provides a comprehensive catalog of security and privacy controls for information systems and organizations.

  - **SP 800-61**, Incident Response Recommendations and Considerations for Cybersecurity Risk Management.
    Assists organizations with incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities that help organizations prepare for incident responses, reduce the number and impact of incidents

that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities.

- **SP 800-171**, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
  Provides recommended security requirements to federal agencies for protecting the confidentiality of controlled unclassified information when the information resides in nonfederal systems and organizations.

- **Cyber Security Framework (CSF).**
  Designed as a flexible framework to be tailored to aid organizations in managing and reducing their cybersecurity risks.

- **Federal Information Processing Standard (FIPS) 199**, Standards for Security Categorization of Federal information and Information Systems.
  Establishes security categories of information and information systems that an organization should assess the risk related to the confidentiality, integrity, and availability categories and then rating each system as "low," "moderate," or "high" impact in each category.

- **Center for Internet Security (CIS)**, Critical Security Controls.

  CIS is an IT community-driven nonprofit organization that provides best practices for securing IT systems and data. Its Critical Security Controls are designed to strengthen an organization's cybersecurity posture through a prescriptive, prioritized set of best practices to defend against the current top cybersecurity threats and to protect systems and networks against cyberattacks.

- **Internal Revenue Services**, Publication 1075, Tax Information Security For Federal, State and Local Agencies.

  Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or sub-contractors adequately protect the confidentiality of federal tax information (FTI).

- **ISACA, COBIT (Control Objectives for Information and Related Technology) Framework.**

  ISACA is a global professional association that provides IT guidance, credentials, education, and training. ISACA's COBIT Framework is designed to facilitate IT governance principles for organizations in the areas of development, improvement, implementation, and management of IT.

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 objective, are described in the remainder of this report and the confidential report.

Drafts of the public and confidential reports were reviewed by OIT. Obtaining the views of responsible officials is an important part of the Office of the State Auditor's (OSA) commitment to ensuring that the reports are accurate, complete, and objective. The OSA was solely responsible for determining whether and how to revise the reports, 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 Auditor's Addendums to responses that are inconsistent or in conflict with the audit's conclusions, findings, or recommendations.

Chapter 2
Public Findings

Finding 1 — IT Governance

Overall, IT governance is a structured framework that provides clear roles and responsibilities, streamlines communication, and defines the processes necessary for managing an organization's IT resources. It ensures that IT investments align with business objectives, mitigate risks, and deliver value to the organization. Essentially, IT governance serves as a bridge between an organization's business goals and its IT infrastructure, and provides the people, processes, and technology to ensure an organization's IT supports the organization's strategies and objectives.

OIT Structure

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 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 matters in the State of Colorado, informing the CIO and executive agency leadership of 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 Information Security Office (ISO), which includes offices for Security Operations, Security Architecture, and Security Risk & Compliance. The ISO is responsible for developing and maintaining state security policies, including the Colorado Information Security Policies (CISPs), and providing leadership for state security initiatives. In addition, the ISO is also responsible for monitoring and tracking OIT's progress toward remediating audit recommendations, and OIT management has assigned this process to the ISO's Security Risk & Compliance Team (Team). The Team tracks audit recommendations and obtains implementation statuses and documentation from OIT's various divisions to support OIT's dispositions, and provides them to the external auditors.

Information Security Policies, Standards, Procedures, and Guidelines

Policies, such as the CISPs, serve as high-level requirements that outline an organization's overall approach and stance on specific risks and controls, defining the **"what"** and **"why"** behind actions and decisions, while establishing management's expectations and guiding principles. An

organization's information security policy is a key component to effective IT governance and risk management. When properly established and enforced, an information security policy helps to create a secure framework that protects the organization's information, resources, and reputation.

In addition, standards establish the minimum-security requirements necessary to effectively protect data and address potential risks and vulnerabilities, while ensuring that systems, processes, and technologies align with industry-leading standards and regulatory expectations. By defining and enforcing these security expectations, standards enable organizations to comply with legal frameworks and proactively mitigate security risks and potential threats.

Lastly, in addition to policies and standards, well-defined and enforced procedures and guidelines are essential for creating a structured and reliable security framework to safeguard sensitive data and information. Procedures and guidelines provide comprehensive, step-by-step instructions that guide staff in performing specific tasks or responding to security scenarios, ensuring tasks are completed consistently and correctly across the organization. Where, as previously described, policies establish the "what" and "why," procedures establish the **"how"** of implementing the policies, translating high-level requirements and expectations into actionable steps that empower employees to effectively manage security processes and maintain operational integrity.

Together, policies, standards, procedures, and guidelines form the foundation of effective governance and risk management, and support a comprehensive and resilient information security strategy, ensuring the confidentiality, integrity, and availability of information and systems while supporting the organization's overall mission and operational goals.

Roles and Responsibilities

Agencies should establish and assign an individual as a primary point of contact for each system at the agency, to fill a key role in the implementation and management of security for the system. OIT, through its December 2024 Colorado Information Security Policies Glossary (CISP Glossary), states that the agency is the data steward and has the authority to authorize or deny access to the data, and is responsible for the accuracy, integrity, and timeliness of the data. OIT provides IT services to the consolidated agencies, in the role of technology provider. The IT roles and responsibilities of the agencies and OIT are outlined within the CISPs, which were most recently released in December 2024, and were enforceable as of July 1, 2025.

At the end of our audit, we became aware that OIT issued updated CISPs, effective November 2025 and enforceable July 2026. OIT consolidated the 16 December 2024 CISPs down to four (4) CISPs that make up the November 2025 CISPs. The November 2025 CISPs were not effective during this audit and therefore were not included with our audit procedures performed during this audit; however, OIT appears to have removed even more specificity, and in turn, may be providing less direction to the consolidated agencies that rely on OIT, as the State's centralized Technology Provider, to provide this direction.

What was the purpose of the audit work and what audit work was performed?

The purpose of the audit work was to determine whether OIT implemented the OSA's May 2023 audit report recommendations related to IT Governance. At the time of the May 2023 audit, OIT disagreed with Part A and did not plan to implement it, but either fully or partially agreed with Parts B–H.

OIT's prior audit recommendations related to IT Governance from our May 2023 audit are listed, as follows:

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 (May 2023 audit report), 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.

To conduct our audit work, we obtained and reviewed supporting documentation provided by OIT management and staff for the parts of the recommendations that OIT had:

- Either "agreed" or "partially agreed" to implement in the May 2023 Audit Report; and
- Indicated it had either "implemented" or "partially implemented" by June 2025, during our current audit.

What problems did the audit work identify and how were the results measured?

We found that OIT, overall, only **partially implemented** the IT Governance recommendations from the May 2023 audit. Specifically, we determined the audited dispositions noted below, with additional explanations for each area.

- Recommendation Part B: **Partially Implemented**

  In OIT's May 2023 audit recommendation response, management partially agreed with Part B, stating that it was transitioning from three levels to four tiered levels of system categorizations (Tiers 1–4) that bases the categorization on how important the system's availability is to the agency's mission. During this audit, OIT reported to us that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had only **partially implemented** this recommendation.

  During this audit, OIT established a tiered approach, based on the availability of the system, as defined by the agency. Specifically, the Tiers are defined as follows:

  - Tier 1—If the application is unavailable, it would create a risk to human life.
  - Tier 2—If the application is unavailable for hours, it would create a significant risk for the agency's performance of its mission.
  - Tier 3—If the application is unavailable for days, it would create a significant risk for the agency's performance of its mission.
  - Tier 4—If the application is unavailable for extended periods of time, even though this is not the intention, it would not create a significant risk for the agency's performance of its mission.

However, we found the following problems with OIT's effort to prioritize information systems across all consolidated agencies:

- OIT did not provide sufficient documentation to demonstrate that it coordinated with and involved the agencies, formally referred to in OIT's March 2022 CISPs as "Business Owners," in the prioritization of their systems to meet the new tiered approach. Although OIT provided a meeting agenda for the OIT Customer User Group—a group created by OIT to include agency representatives and OIT staff—dated June 13, 2024, the meeting agenda failed to include the attendees or any notes taken during the 15 minutes of the meeting dedicated to discussing the tiered approach.

- OIT did not provide documentation that it conducted additional prioritization procedures within each tier, and in coordination with agency staff, to provide essential direction to OIT and agency staff responsible for conducting security risk assessments, developing system security plans, and testing system recovery efforts when a major incident or disaster occurs, or when systems need security updates.

We measured the results of our audit work against the following specific criteria:

- NIST, SP 800-53, Rev 5, states the following:

  - CP-2(8), organizations should identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources.

  - RA-2(1), organizations should conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

  - RA-9, organizations should 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.

- NIST, SP 800-37, Rev 2, Task P-10, states that the organizations—OIT and the agencies, in this case—define the scope of the assets to be considered for protection. The assets that require protection should be identified based on OIT's and the agencies' concerns and the contexts in which the assets are used. This includes the missions or business functions of the agencies, the other systems that interact with the system, and those whose assets are utilized by the mission or business functions or by the system.

- Green Book states the following:

  - Attribute 3.09 states that that management should develop and maintain documentation of its internal control system.

- Attributes 3.10 and 3.12 state that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external auditors, and to ensure internal controls are designed, implemented, and operating effectively.

- Attribute 7.06 states that management should estimate the significance of risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk.

- Attributes 15.03 and 15.04 state that management should communicate quality information externally so that external parties can help the entity achieve its objectives and address related risks, which is necessary for the effective operation of internal controls.

- Recommendation Part C: **Partially Implemented**

  During this audit, OIT reported to us that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had only **partially implemented** this recommendation.

  OIT drafted a standard operating procedure (SOP), Communicating New or Updated Office of Information Security (ISO) Policies, Standards and Forms, stating the SOP's purpose was to create "a uniform process for communicating new and/or updated policies and standards promulgated" by the CISO and ISO. The SOP, which was last updated on June 30, 2025, includes various methods for how the CISO and the ISO will communicate updates of policies, standards, and forms, both internally and externally.

  However, we found the following problems with the SOP:

  - The SOP did not contain an effective date for when it was implemented or any evidence that it had been reviewed and approved by someone at a management level to ensure it met management's expectations.

  - The SOP does not formalize the distinction between, or define, the "effective date" versus the "enforcement date," which are two different dates that OIT included, for the first time, within the December 2024 CISP updates. We were also unable to find the distinction between the meaning of these two dates formalized within any of the December 2024 CISPs. Further, the SOP notes that "Absent extenuating circumstances, the effective date of the new or updated policy or standard is timed to coincide with the weekly OIT Employee Bulletin. This allows for timely communication using existing channels for sharing information with OIT employees." With this statement, one might interpret it to mean that the CISPs and OIT standards are "effective" on a weekly basis, when these communications occur, rather than, or regardless of, any "enforcement" dates noted in them, which may be confusing to OIT staff.

  - The SOP contained outdated terminology and information. For example, we found that:

- One non-consolidated agency contact listed in the SOP had been retired for more than a year prior to the last SOP review date of June 30, 2025.

- Even though OIT has established an annual review, through the Using ServiceHub Knowledge for OIT's Knowledge Management System policy, for all OIT knowledge documents, such as SOPs, it referenced other documentation from Fiscal Year 2021 related to the CISP review process with a date over four years old, which may indicate that the SOP had not been reviewed in accordance with management's expectations.

- Although the CISPs prior to the March 2022 CISPs included a definition of the purpose of the CISPs as providing minimum security requirements for "low" or "moderate" protected data, these specific distinctions were removed from the March 2022 CISPs and also were not included in the December 2024 CISPs.

OIT stated, based on our follow-up inquiries related to the problems we noted, that the SOP was being updated and would be completed by October 2025.

OIT also provided a policy update schedule that outlines OIT's "activities that are needed to successfully deliver policies on an annual basis." Each tab of the spreadsheet establishes the "activities" and the associated timelines, between January and December each year, including when policies are enforceable and when they are retired. We noted that one specific "activity" listed for the policy enforcement tab was to "Track compliance to policies on a monthly basis." However, it was unclear who within the ISO is responsible for this compliance tracking. Further, another "activity" listed was to "Work with Exec staff on appropriate sanctions for continued non-compliance." Again, we were unclear whether sanctions would apply only to OIT staff's noncompliance or if it also included consolidated agencies' staff noncompliance.

In addition, when we reviewed the December 2024 CISPs, each policy contained the same information in regards to the agency being "responsible for contracting for security and compliance and that there is a validation of compliance." However, C.R.S., 24-37.5-403(c) and (d) establish that the CISO is responsible for ensuring public agencies comply with security policies and they can also direct information security audits and assessments. Although it seems that OIT may be attempting to transfer its statutory responsibility to direct information security audits and assessments to the agencies through policy, OIT did not respond to our direct question of whether the CISO was transferring this responsibility. While OIT provided documentation that the CISO's ISO staff had conducted a limited number of risk assessments on agency contractors, OIT did not provide us any documentation that the ISO staff had conducted any information security audits and assessments at any of the consolidated agency, to ensure the agency was in compliance with the agency specific December 2024 CISP requirements. Further, OIT did not clarify its position to us on the statutory responsibility and provided no further explanation about whether the CISP security and compliance requirement, and the statutory requirement were directly related. Lastly, OIT did not provide any procedural documentation as to how OIT will ensure the agencies are complying with the CISP contracted

security compliance validation requirement and that OIT is aware of any noncompliance from these validations.

OIT's only response to our inquiries, related to this recommendation and the documentation they provided, was to say that it had removed the "Track compliance to policies on a monthly basis activity" from the policy update schedule, but did not provide a revised policy update schedule to demonstrate that it removed this "activity."

We measured the results of our audit work against the following specific criteria:

- Sections 24.37.5.403(c) and (d), C.R.S., state that the CISO shall ensure compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies—in this case the Enterprise Cyber Security Plan prepared by OIT's ISO for the consolidated agencies—pursuant to Section 24-37.5-404, C.R.S., in addition to, directing information security audits and assessments in public agencies in order to ensure program compliance and adjustments.

- CISP-017, IT Security Planning, Section 5.5, states that the agency is responsible for contracting for security and compliance and that there is a validation of compliance.

- POL-OIT: Using ServiceHub Knowledge for OIT's Knowledge Management System states that to ensure that knowledge content is complete, accurate, and relevant, the following practices are enforced:

  - All articles, or documents, have a "Valid to Date" that is set to 12 months by default. As a result, all articles will be reviewed, at least, on an annual basis. The timeframe for review can be shortened, but cannot exceed 12 months.

- Green Book states the following:

  - Attribute 3.09 states that that management should develop and maintain documentation of its internal control system.

  - Attributes 3.10 and 3.12 state that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external auditors, and to ensure internal controls are designed, implemented, and operating effectively.

  - Attribute 7.06 states that management should estimate the significance of risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk.

  - Attribute 10.02 states that management designs control activities, such as procedures, in response to the entity's objectives and risks to achieve an effective internal control system. In addition, procedures aid the entity in achieving its objectives, fulfill defined responsibilities, and address identified risk responses.

- Attribute 10.03 states that management divides or segregates key duties and responsibilities so that no one individual controls all key aspects of a process.

- Attributes 15.03 and 15.04 state that management should communicate quality information externally so that external parties can help the entity achieve its objectives and address related risks, which is necessary for the effective operation of internal controls.

- Component OV2.15 states that external auditors are not considered a part of an entity's internal control system, rather the responsibility resides with the entity's management.

- Recommendation Part D: **Partially Implemented**

  During this audit, OIT reported to us that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had only **partially implemented** this recommendation.

  We found the following problems with the documentation and responses OIT provided to support its implemented disposition:

  - OIT did not provide sufficient documentation to demonstrate that it implemented the part of the recommendation stating, "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." While OIT published updated CISPs in December 2024 that replaced the term "Business Owner" with "Agency," OIT did not provide documentation that definitions had been updated and/or clarified within the information security programs or plans. OIT indicated that it updated its "communication plans and associated materials," but our request for these documents was not fulfilled. Additionally, OIT provided a communication stating that agency product directors were involved in reviewing the draft CISPs, prior to the December 2024 release, but the communication OIT provided to us was only a partial screenshot, which did not provide information such as the sender, the date sent, and details of who the agency product directors are and the role they played in the clarification of the business owner role change to the consolidated agencies.

  - OIT included inconsistent or outdated terminology within its CISP Glossary, which defines terms used in the December 2024 CISPs. Within the December 2024 CISPs, OIT included a definitions section, in which OIT states, with exception of any unique definitions included in each CISP, the reader should refer to the CISP Glossary. Specifically, and as it relates to the CISP Glossary, we found the following:

    - Agency or Agencies—OIT included these terms, and in defining them, referred to the statutory definition of "public agencies" [C.R.S., 24-37.5-102(26)], which is the same definition OIT includes in the Scope/Organizations Affected section in each December 2024 CISP. Therefore, OIT had not provided a clear definition of Agency or Agencies to describe their IT roles, responsibilities, or any other IT related information that would

ensure a reader, such as IT staff within the consolidated agencies, would understand the "who, what, and why," of an Agency or Agencies role(s) in relation to the CISPs and IT in the State.

- Technology Provider—OIT did not include nor define this term in the CISP Glossary that replaced "IT Service Provider" in the December 2024 CISPs.

- Business Owner and IT Service Provider—Although both terms were included and defined in the 2024 Glossary, neither were found within the December 2024 CISPs, as OIT replaced Business Owner with Agency and IT Service Provider with "Technology Provider."

- Technical Owner was included with an OIT explanation for how it addressed this recommendation, but this term was not defined in the CISP Glossary.

Based on our inquiries, OIT updated the CISP Glossary in June 2025 to revise the definitions of Agency, removed Business Owner, and also revised IT Service Provider, as well as by adding Technology Provider. However, these updates occurred 6 months after the December 2024 CISPs were published and effective and after we inquired about them. OIT stated that the use of Technical Owner in its responses to our inquiries was used in error, is not a current term, and should not be defined in the CISP Glossary.

◦ OIT did not respond to our questions nor provide documentation to demonstrate how it implemented the part of the recommendation stating, "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."

We measured the results of our audit work against the following specific criteria:

◦ Green Book states the following:

- Attribute 3.06 states that in order to achieve the entity's objectives, management should assign responsibility and delegate authority to key roles throughout the entity. A key role is a position in the organizational structure that is assigned an overall responsibility of the entity.

- Attribute 3.09 states that management should develop and maintain documentation of its internal control system.

- Attributes 3.10 and 3.12 states that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external auditors, and to ensure internal controls are designed, implemented, and operating effectively.

- Attribute 14.03 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.

- Attributes 15.03 and 15.04 state that management should communicate quality information externally so that external parties can help the entity achieve its objectives and address related risks, which is necessary for the effective operation of internal controls.

- Component OV2.15 states that external auditors are not considered a part of an entity's internal control system, rather the responsibility resides with the entity's management.

- Recommendation Part E: **Partially Implemented**

  During this audit, OIT reported to us that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had only **partially implemented** this recommendation.

  We determined that OIT implemented the May 2023 audit's confidential Asset Management Recommendation Parts A and B, referenced in this Recommendation Part E. As to the second part of the recommendation—"working with agencies to identify Business Owners for all applications management by OIT and ensuring these roles are consistently defined in system security plans and system inventories"—OIT did not provide sufficient documentation to support that it implemented the recommendation. More specifically, we found the following:

  - Although OIT's Senior IT Director stated that OIT had worked with the agencies to "emphasize the importance of having Ownership information up-to-date in ServiceHub," they continued to use the term, Business Owner in their response, even though OIT had updated Business Owner with Agency in its December 2024 CISPs.

  - OIT only provided documentation of business applications for one consolidated agency and itself, but not for the remainder of the consolidated agencies. Also, when reviewing the documentation, we noted that the documentation also continued to use the term Business Owner.

  - OIT did not provide documentation that it had ensured these roles were consistently defined in system security plans.

  We measured the results of our audit work against the following specific criteria:

  - NIST, CSF 2.0, GV.RR, states that an organization should establish and communicate the cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement.

- COBIT Framework 2019, Governance and Management Objectives, APO01.07, states that organizations—in this case, OIT and agencies— should define and maintain responsibilities for ownership of information (data) and information systems; and create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications.

- Green Book states the following:

  - Attribute 3.09 states that management should develop and maintain documentation of its internal control system.

  - Attributes 3.10 and 3.12 state that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external auditors, and to ensure internal controls are designed, implemented, and operating effectively.

  - Attribute 14.03 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.

  - Attributes 15.03 and 15.04 state that management should communicate quality information externally so that external parties can help the entity achieve its objectives and address related risks, which is necessary for the effective operation of internal controls.

- Recommendation Part F: **Not Implemented**

  During this audit, OIT reported to us that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had **not implemented** this recommendation.

  Overall, OIT's responses to this recommendation, starting with its May 2023 audit response to those obtained during our current audit, have been unclear as to how OIT will address the risk related to agencies not receiving necessary training to understand and articulate the security requirements that they are responsible for and for which OIT, as the consolidated agencies' Technology Provider, may need to implement for any given agency owned system. For example, according to CISP-017, Section 6.2, System Security Plans (SSPs or plan), "The Agency owns the plan;" however, OIT indicated that security responsibilities are solely assigned to the ISO staff. Therefore, the SSP requirement that the agencies own the plans, but only ISO staff are assigned security responsibilities and obtain security requirements training, despite there being numerous security responsibilities delegated to the agencies in the CISPs, is inconsistent with OIT stating in its June 30, 2025, response that the risk no longer exists, and especially when state statute requires the CISO to ensure compliance with information security policies.

Since we have made recommendations to OIT, through Recommendation 2, Security Training and Awareness, that would also address this recommendation, we are not including another related recommendation in this finding. (See Recommendation 2, Security Training and Awareness.)

We measured the results of our audit work against the following specific criteria:

- Green Book states the following:
  - Attribute 3.09 states that that management should develop and maintain documentation of its internal control system.
  - Attributes 3.10 and 3.12 states that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external auditors, and to ensure internal controls are designed, implemented, and operating effectively.

- Recommendation Parts G and H: **Partially Implemented**

  During this audit, OIT reported to us that these recommendations were implemented by June 30, 2025. However, we determined based on our audit work that OIT had **partially implemented** these recommendations.

  OIT began drafting and/or updating its Technical Standards, which they stated would define minimum security requirements, instead of including these requirements in the CISPs, as was the case in past versions of the CISPs, prior to March 2022. However, despite OIT indicating that this recommendation has been implemented, not all Technical Standards OIT reported as updated were published in ServiceHub and on OIT's website by June 30, 2025.

  We also reviewed OIT's website on two different dates, July 9 and July 15, 2025, and noted that six CISO-specific Technical Standards were noted as "expired." We inquired with OIT regarding the status of these six Technical Standards, as it was unclear whether "expired" meant that the Technical Standard was in the process of being reviewed, but OIT did not directly address our request for clarification on these. We then noted on July 29, 2025, that OIT's website stated these six were "retired." Further, OIT provided a "CISO Technical Standard" tracking spreadsheet that included seven new Technical Standards, but these were not posted to OIT's website as of July 29, 2025. We also encountered problems with OIT providing documents that appeared to be new Technical Standards, which were also listed on its tracking spreadsheet, as they were similar in nature to those that OIT had "retired" after our initial inquiries. However, OIT did not respond to our follow-up questions to clarify whether the documents were, in fact, current Technical Standards.

  Additionally, we noted during our review of the Technical Standards documents that OIT provided, and those that appeared to be Technical Standards from the document title, that minimum security requirements were not included in certain Technical Standards. In those

instances, OIT reported that the requirements would be included in separate "operating standards," but OIT did not provide documentation to verify those statements for all instances we inquired about, and OIT did not communicate to us which Technical Standards would include the minimum security requirements for session time outs and backup frequencies.

OIT also provided updated Technical Standards, in some instances, that did not identify the Technical Standard's owner or author and a management level review and approval, an effective date, and revision history. In other instances, OIT did not provide complete and accurate Technical Standards and, instead, either did not provide an updated Technical Standard to address our questions or stated they were still in the process of updating the Technical Standard. At that time, OIT also reported that the Technical Standards in question would be updated and posted to OIT's website by September 2025, rather than by June 30, 2025, which was OIT's planned implementation date.

OIT established the Standard Operating Procedure for Creating, Updating, and Implementing Standards (SOP) that was formalized to "provide a uniform process for creating, reviewing and approving, updating, and implementing, and enforcing technical standards." Specifically, the SOP establishes an annual review process; however, the SOP is not clear on what the "annual" review date is based on and whether there is a minimum time between reviews, if, for example, there are no significant changes prior to the next, annual review. Further, we were unable to determine who owned or authored the SOP and who at a management level reviewed and approved it, as well as an effective date and revision history.

We measured the results of our audit work against the following specific criteria:

- OIT's SOP for Creating, Updating, and Implementing Standards indicates, in the process for new Technical Standards—specifically steps 11a and 11b—that the Architecture Review Board (ARB) members review and determine if the standard is approved and, if so, the requester will upload the standard into ServiceHub and the ARB Chair will be the final approver of the standard. Then, OIT's Communication Office will add the standard to the Technical Standards and Policies page on OIT's public website.

  Further, this SOP defines that a technical standard should include detailed specifications that contain measurable, mandatory requirements to be applied to an information technology process, system, or action. OIT develops technical standards to ensure consistency and reliability of methods and services used by OIT and state agencies.

- Green Book states the following:

  - Attribute 3.09 states that management should develop and maintain documentation of its internal control system.

  - Attributes 3.10 and 3.12 state that effective documentation of an entity's internal control system is a means to communicate knowledge to external parties, such as external

auditors, and to ensure internal controls are designed, implemented, and operating effectively.

- Attribute 16.04 states that management should monitor the internal control system through ongoing monitoring.

- Attribute 17.06 states that management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

Why did these problems occur?

Overall, we found that OIT's implementation of our IT Governance recommendations was either still in process at the time of our audit or that OIT considered the recommendations to be implemented, despite being unable to provide sufficient documentation to demonstrate it had, in fact, implemented the recommendations related to improving its IT governance controls for the consolidated agency systems it manages.

In addition, the problems we noted point to OIT lacking an effective system of internal control and raises the risk of OIT providing inaccurate and incomplete information, both internally and externally. The design and implementation of OIT's controls, including the tracking, monitoring and providing of documentation that supports implementation of its audit recommendations, should be clear of unnecessary or inaccurate information. Further, external auditors should not act as part of an entity's system of internal control.

Lastly, OIT did not effectively communicate to or train staff regarding the importance of utilizing updated, or current, terminology consistently in all forms of communication and within documentation, to reduce any confusion, when they are interacting with both internal and external parties.

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 prioritization of agency information systems; setting of policies standards, and procedures; defining roles and responsibilities; and effective communications. For instance, without prioritization of information systems, OIT cannot ensure it effectively utilizes its time and resources across all of its initiatives. In turn, this may impact the life and safety of Colorado citizens. Examples of this would be a large-scale outage where multiple mission critical systems need to be restored. Without agreed-upon prioritization, all agencies might indicate that their information systems are most critical and expect, or demand, 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 activities such as developing system security plans or conducting system risk assessments may continue to be a struggle for OIT to accomplish without proper system prioritization.

Since perceptions and understanding of security vary, these activities provide expectations and guidelines to those responsible for implementing and managing security to ensure consistency throughout OIT and the State. Without these aspects of governance and oversight, IT security may be erratically applied across organizations and systems. As a result, overall security is reduced as there may be confusion about 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.

Also, without proper monitoring controls, management may not be able to ensure that audit recommendations are addressed and resolved in a timely manner. In addition, without controls that are established and communicated to ensure competencies are defined, delegations are documented, and duties are segregated, staff roles may not be clearly understood. Ultimately, the lack of security controls increases the risk to the confidentiality, integrity, and availability of the impacted systems and their data, and may prevent organizations from properly managing and mitigating the risks associated with cyber threats.

Recommendation 1

The Governor's Office of Information Technology (OIT) should improve IT governance, including its overall system of internal controls, by:

A. Ensuring its audit recommendation tracking and monitoring process is effective so that OIT implements audit recommendations in a timely manner. This process should include OIT staff providing complete and accurate documentation.

B. Conducting additional prioritization procedures within each tier, in coordination with consolidated agencies, that results in providing essential direction to OIT and agency staff responsible for conducting security risk assessments and the development of system security plans and system recovery efforts when a major incident or disaster occurs, or when systems need security updates. Once completed and ongoing, OIT should maintain documentation of its related processes.

C. Updating the Communicating New or Updated Office of Information Security Policies, Standards, and Forms standard operating procedure to clarify its expectations related to effective dates; management approvals; distinguishing the difference between "effective date" and "enforcement date," as it relates to the dates included in OIT's Colorado Information Security Policies (CISPs); and removing outdated information and terminology.

D. Determining whether the CISP requirement for agencies being "responsible for contracting for security and compliance and that there is a validation of compliance" is in compliance with the CISO's statutory requirement [Section 24.37.5.403(c)and (d), C.R.S.] to ensure public agencies comply with security policies through direct information security audits and assessments. Based on this determination, updating the CISPs accordingly, and formalizing related processes to

conduct the audits and assessments to adhere to Colorado Revised Statutes and the updated CISPs.

E. Finalizing processes to ensure its setting, documenting, and communicating a clear and consistent definition for the role of Agency throughout the State's information security programs, policies, and plans. This should also include differentiating between enterprise-level, agency-level, and system level ownership when referring to the roles and responsibilities of an agency and ensuring these roles are consistently defined in security programs and system security plans. Once these steps are complete, OIT should maintain supporting documentation of this process and its results.

F. Ensuring the CISPs Glossary includes accurate and up-to-date information.

G. Ensuring that OIT staff are trained on and utilize current CISP terminology, which will aid in establishing consistency and reducing confusion in all forms of communication and within documentation, when they are interacting with both internal and external parties. This training should occur when significant terminology changes are made to future versions of the CISPs.

H. Maintaining documentation to support that OIT worked with agencies to identify agency ownership for all applications managed by OIT and ensuring that these roles are consistently defined in system security plans and system inventories.

I. Updating the Standard Operating Procedure for Creating, Updating, and Implementing Standards (SOP) to ensure OIT's Technical Standards that are posted to its public website include an owner or author and a management level review and approval, an effective date, revision history, and a standard numbering sequence. In addition, updating the SOP's annual review process to clarify what the annual review date is based on and whether there is a minimum time between reviews.

J. Ensuring management's expectations are implemented by documenting minimum security standards within the Technical Standards and ensuring that the Technical Standards are published appropriately and in a timely manner once they are documented, reviewed, and approved in accordance with the SOP noted in Recommendation Part I.

Response

Governor's Office of Information Technology

A. Partially Agree
Implementation Date: June 2026

OIT disagrees with the recommendation's specific focus on implementing "audit recommendations." In accordance with Green Book Principle 17, management is responsible for evaluating issues and determining the appropriate corrective actions to remediate internal control deficiencies. Therefore, OIT will focus its process on remediating and addressing the

risk from audit findings. This ensures corrective actions effectively mitigate identified risks while allowing OIT to adapt to changing organizational priorities.

Auditor's Addendum

As noted in the finding, we found that OIT lacked an effective system of internal control. More specifically, we noted that OIT failed to effectively document its design and implementation of its audit recommendation tracking and monitoring, controls that supports implementation of its audit recommendations, in a timely manner. Green Book specifically states that management should complete and document corrective actions to **remediate internal control deficiencies on a timely basis, and that corrective actions include the resolution of audit findings** [emphasis added].

B. Disagree
Implementation Date: Not Applicable

Business criticality tiers are determined in collaboration with the agency Product Directors. The criticality tiers are used to prioritize risk assessments.

Auditor's Addendum

As noted in the finding, OIT did not provide sufficient documentation to demonstrate that it coordinated with and involved the agencies to further prioritize systems within each tier. Without this further prioritization of systems, OIT cannot ensure it effectively utilizes its time and resources across all of its initiatives, it may impact the life and safety of Colorado citizens, and all agencies might indicate that their systems are most critical and expect, or demand, services to be restored first, in the event of major incident or if a disaster occurs.

C. Agree
Implementation Date: June 2026

OIT will update the document to explicitly define effective date versus enforceable date, ensure proper management approval, and remove outdated terminology.

D. Partially Agree
Implementation Date: July 2026

The referenced language is not included in the current CISPs. In addition, OIT meets the requirements of C.R.S. 24-37.5-403 (d). OIT is partnered and actively working with non-consolidated agencies to update the rules in order to adhere with C.R.S. 24-37.5-403 (c).

Auditor's Addendum

As noted in the finding, OIT did not respond to our direct inquires or provide any documentation related to the December 2024 CISPs requirement that agencies are "responsible for contracting for security and compliance and that there is a validation of compliance," and

whether the CISO was transferring its statutory responsibility outlined in Section 24-37.5-403(d), C.R.S., requiring OIT, specifically the CISO to "direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments." Therefore, it is unclear how OIT is meeting the statutory requirements in Section 24-37.5-403(d), C.R.S.

Further, Section 24-37.5-403, C.R.S., refers to "public agencies," which is defined in statute as including the consolidated agencies, the non-consolidated agencies of the Departments of Education, Law, State, and Treasury, and the judicial branch agencies, but does not include the institutions of higher education or the legislative branch agencies. Therefore, it is unclear why OIT is indicating it is only "partnered and actively working with non-consolidated agencies," instead of also including the consolidated agencies, since they are included in the statutory definition of "pubic agencies." Overall, statute requires that OIT, and the CISO specifically, must ensure compliance with information security policies, standards, and guidelines for public agencies.

E. Disagree
Implementation Date: Not Applicable

Continuous improvement efforts will refine and mature OIT in this area.

Auditor's Addendum

Based on OIT's response, it is unclear what OIT is disagreeing with in the recommendation, and how it will address the risk related to not setting, documenting, and communicating a clear and consistent definition for the role of agency throughout the State's information security programs, policies, plans, and differentiating between enterprise-level, agency-level, and system level ownership when referring to the roles and responsibilities of the agencies.

F. Partially Agree
Implementation Date: December 2026

OIT acknowledges the recommendation and recognizes that inconsistent or outdated terminology contributed to confusion across CISPs and supporting documentation. While the CISP Glossary is not intended to be the long-term system of record for OIT terminology, OIT is determining the appropriate processes and governance model for maintaining a standard language library and ensuring that CISPs and related documentation reference current, consistent terminology. The specific approach and implementation are under evaluation and a documented timeline is expected by December 2026.

Auditor's Addendum

Based on OIT's response, it is unclear what OIT is disagreeing with in the recommendation. As noted in the finding, OIT continued to use outdated terminology in the documentation it provided to us during the audit and in responding to inquiries, but then updated its documentation, only after our inquiries. Our recommendation is that OIT should ensure that

it has processes in place to routinely update its Glossary going forward. See also Recommendation 1, Part G.

G. Partially Agree
Implementation Date: December 2026

OIT acknowledges the recommendation and recognizes that inconsistent or outdated terminology contributed to confusion across CISPs and supporting documentation. While the CISP Glossary is not intended to be the long-term system of record for OIT terminology, OIT is determining the appropriate processes and governance model for maintaining a standard language library and ensuring that CISPs and related documentation reference current, consistent terminology. The specific approach and implementation are under evaluation and a documented timeline is expected by December 2026.

Auditor's Addendum

As noted in the finding, senior OIT staff continued to use outdated terminology, in written responses to our inquiries during the audit, more than 6 months after the release of the December 2024 CISPs. Further, our recommendation is for OIT to provide staff training on CISP terminology to assist in ensuring that staff use the current terminology, which will aid in establishing consistency and reducing confusion in all forms of communication and within documentation when they are interacting with both internal and external parties. However, OIT's response does not specifically address training staff. See also Recommendation 1, Part F.

H. Partially Agree
Implementation Date: December 2026

Supporting documentation to meet compliance requirements is maintained to meet the relevant federal framework.

OIT will continue to work with agencies to ensure ownership is consistent with application documentation.

Auditor's Addendum

As noted in the finding, OIT only provided documentation of business applications for one consolidated agency and itself, but not for the remainder of the consolidated agencies, and did not provide documentation that it had ensured these roles were consistently defined in system security plans.

I. Partially Agree
Implementation Date: July 2026

The SOP will be updated to require all necessary details within Technical Standards. The annual review process will also be clarified regarding frequency and baseline dates.

Auditor's Addendum

Based on OIT's responses, it is unclear what OIT is disagreeing with in the recommendation.

J. Agree
Implementation Date: September 2026

OIT will ensure minimum security standards are documented within Technical Standards and published after documentation, review, and approval, utilizing the updated SOP noted in Part I.

Finding 2 – Information Security Training and Awareness

As indicated in its Colorado Information Security Policy (CISP), titled CISP-002, IT Security Awareness Training (effective December 2024), 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 are required to read and sign their acknowledgement of annually. The Information Security Office (ISO), within OIT, is responsible for ensuring that all OIT personnel complete information security training on an annual basis. In addition, ISO periodically distributes training materials to consolidated agencies, but agencies are responsible for ensuring the security training is completed by all personnel. CISP-002 requires all users to participate in security awareness training annually.

What was the purpose of the audit work and what audit work was performed?

The purpose of the audit work was to determine whether OIT implemented the May 2023 audit report recommendations related to information security training and awareness, including compliance with OIT's Acceptable Use Policy. The May 2023 audit recommendations that OIT partially agreed to implement were to 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 CISPs. Note: OIT replaced the term "Business Owner" with "Agency" in the CISPs, as of December 2024.

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.

To conduct our audit work, we obtained and reviewed supporting documentation provided by OIT management and staff for the parts of the recommendations that OIT had:

- Either "agreed" or "partially agreed" to implement in the May 2023 Audit Report;
- Either "partially implemented" or "not implemented," as of OIT's July 2024 Status Report (as substantiated by the OSA); and
- Indicated it had either "implemented" or "partially implemented" by June 2025, during our current audit.

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

We found that OIT, overall, only **partially implemented** the information security and awareness recommendations from the May 2023 audit. Specifically, we determined the audited dispositions noted below, with additional explanations for each area.

- Recommendation Parts A and B: **Not Implemented**

  In OIT's May 2023 audit recommendation response, management agreed to implement the recommendation by working with Business Owners, its IT Directors, and a vendor to establish specific role-based training options, stating, "…role-based training is lacking and we are working on those options," and that "role based training can and should be improved so that all roles within OIT understand their responsibilities around cyber security." OIT provided a June 2025 implementation date. In OIT's July 2024 Status Report, OIT management reported that these recommendations were not implemented and updated its implementation dates to indicate it would be implementing the recommendations earlier than June 2025—in December 2024. Subsequently, OIT reported to us during this current audit that this recommendation was not implemented by June 30, 2025, and OIT stated that it does not plan to implement what it originally agreed to implement. Therefore, we determined based on our audit work that OIT did **not implement** this recommendation.

  OIT indicated that information security responsibilities are assigned to OIT's ISO and its staff only and are not delegated to Business Owners or other individuals in the organization and that, as a result, no specific training is required for Business Owners or OIT's IT Directors regarding their security responsibilities. As a result, OIT stated that it has decided that it will not be creating additional training materials.

  Although OIT stated that only ISO staff have security-related responsibilities, we found that this is inconsistent with OIT's CISPs. Specifically, CISPs require various security-related responsibilities for the "Agencies." As an example, CISP-001, IT Access Control Management and User Security, Section 6.2, specifies the following for Access Control Management:

- The Technology Provider and **Agency** [emphasis added] must:
    1. Manage IT asset access
    2. Require multifactor authentication (MFA) on all administrative accounts and for all remote access
    3. Ensure the data is transmitted securely to only authorized recipients
    4. Display security logon banner

These are clearly information security responsibilities that OIT has assigned to the Agencies (formerly Business Owners) through its CISPs, and they are one example of many other Agency security responsibilities that OIT has specified throughout the CISPs.

As it relates to OIT's IT Directors, the above referenced policy, CISP-001, also states that the "Technology Provider"—defined in CISPs as OIT, in general, with no specific roles or personnel types defined under it—must fulfill the related security responsibilities noted, in addition to others that are stated for the Technology Provider throughout the CISPs. Overall, since the policy does not explicitly state that only ISO staff have security-related responsibilities, and it excludes IT Directors from being a part of the Technology Provider role, it is unclear whether the IT Directors are, in fact, excluded from security responsibilities, as OIT stated. Further, since OIT has stated that the IT Directors work directly with agencies to ensure customer engagement and delivery, and OIT has assigned specific IT Directors to one or more of the consolidated agencies to carry out their IT functions, it is logical and plausible to think that the IT Directors would have certain security-related responsibilities.

Also, CISP-002, IT Security Awareness and Training, Section 6 Safeguards, states that "Training must be provided at least annually by agencies and Technology Providers." Further, although Section 6.1 states that "The **organization** [emphasis added] must develop a program to conduct security training and awareness programs to include role-based training," the term "organization" is not defined in OIT's CISPs. Thus, it is unclear who the "organization" is and who, ultimately, is responsible for providing role-based security training.

We measured the results of our audit work against the following specific criteria:

- CISP-002, IT Security Awareness and Training, Section 6.1a., states that the organization must develop a program to conduct security training and awareness programs to include role-based training, on at least an annual basis. Section 7.3 states that policy exceptions submitted to OIT must follow OIT's risk management process, which outlines compensating controls, risk mitigation options, and timelines for remediation.

- NIST, SP 800-53, Rev 5, Security and Privacy Controls for Information Systems and Organizations Control, AT-3, states that comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures,

tools, methods, and artifacts for the security and privacy roles defined. Examples of the roles that should obtain role-based training would be senior leaders or management—which would include those at the agencies, those in technical IT roles—which could include OIT's IT directors, and contractors.

- NIST, SP 800-50, Rev 1, Building A Cybersecurity and Privacy Learning Program, Section 2.5. Learning Program Audience Segments, states that users, including contractors, with significant cybersecurity and/or privacy responsibilities, require an individualized program of role-based training to ensure that their knowledge and skills are sufficient to execute the tasks required for their work.

- Green Book, Attribute 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.

- Recommendation Parts C and D: **Partially Implemented**

  In OIT's May 2023 audit recommendation response, management agreed to implement the recommendation by ensuring that OIT staff put in additional effort and focus toward monitoring and enforcing the existing policies and strengthening its tracking, updating, and maintaining its records by its implementation date of December 2023. In OIT's July 2024 Status Report, OIT management reported that these recommendations were not implemented and updated its implementation dates to December 2024. Subsequently, OIT reported to us during this current audit that this recommendation was implemented by June 30, 2025. However, we determined based on our audit work that OIT had only **partially implemented** this recommendation.

  We found that OIT has designed and implemented a process to establish sanctions/corrective actions for those OIT employees and external users that do not complete security awareness training in a timely manner and to complete an Acceptable Use Policy attestation at the time of employment and annually thereafter. However, although OIT reported to us that they fully implemented these recommendation parts, OIT failed to provide documentation that:

  - OIT employees and external users fully complied with the most current year's training and Acceptable Use Policy attestation requirements or, if not, that sanctions/corrective actions, identified within the Business Operating Procedure (BOP)-HR-001, Noncompliance with Required Training, were enforced for OIT employees and external users.

  - OIT IT Directors were working with agency staff to ensure that those at the agency, including agency external users, were being assessed agency-level sanctions for not completing security awareness training and Acceptable Use Policy attestations in a timely manner.

  Further, OIT Human Resources' email communication, dated May 7, 2025, to OIT executive leadership listing OIT employees who failed to comply with the mandatory training

requirements, as required within the BOP, was not clear. Specifically, it did not specify whether the reported information also included noncompliance with OIT's required employees and external users Acceptable Use Policy attestations.

We measured the results of our audit work against the following specific criteria:

- CISP-002, IT Security and Awareness Training, Section 7.2, states that failure to comply with this policy may result in, as applicable, agency-level sanctions regarding state IT resources: restriction, deactivation, or suspension of the project or system.

- CISP-018, Acceptable Use of State Data and IT Resources (Acceptable Use Policy), Section 17, states that this policy must be accepted by users at the start of employment and no less than annually thereafter. CISP-018, Section 18, states that failure of users to comply with this policy may result in, as applicable, agency-level sanctions regarding state IT resources; restriction, deactivation, or suspension of the project or system; or referral to law enforcement. Further, a violation of this policy by temporary workers, interns, volunteers, contractors or vendors may result in termination of their contract or assignment with the State of Colorado. The December 2024 CISP Glossary defines "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."

- OIT's BOP-HR-001: Noncompliance with Required Training, states the following:

  - Purpose—OIT employees are required to complete the required training within the assigned deadlines, in which training has been defined as Cybersecurity/Acceptable Use Policy/Information Security.

  - OIT Managers Responsibilities—Holding his/her staff accountable to comply or follow appropriate corrective and disciplinary processes up to and including termination.

  - OIT Executive Staff Responsibilities—Holding his/her managers accountable to the noncompliance actions, as reported to him/her by Human Resources when employees are 60+ days past due on required training.

- OIT's Monthly Communication Email Template from OIT's Chief Customer Officer and Chief Information Security Officer to OIT's IT Directors—dated March 31, 2025, and would continue monthly on the last day of the month— reports noncompliance with mandatory training and Acceptable Use Policy attestations for the consolidated agencies that each IT Director represents and requires that the IT Directors are to share the information with the agency contact that is responsible for taking action on any noncompliance.

- Green Book, Attributes 5.03 and 5.05, state that management should hold entity personnel and service organizations accountable for performing their assigned internal control responsibilities.

Why do these problems matter?

Educating users and holding them accountable for 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 in accordance with their assigned roles and responsibilities. Further, if OIT and agency-level sanctions/corrective actions are not enforced for OIT and agency employees, including external users, who fail to comply with policy requirements regarding completing security awareness training and Acceptable Use Policy attestations in a timely manner, they may not be held accountable for carrying out management's expectations.

Recommendation 2

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

A. Following its December 2024 Colorado Information Security Policy (CISP) to establish a formal training program for consolidated agencies that outlines and provides necessary direction on their security roles and responsibilities, or revising its current CISPs to otherwise ensure that staff at the consolidated agencies are appropriately trained on their security roles and responsibilities.

B. Following its December 2024 CISPs to establish a formal training program for OIT's IT Directors that outlines and provides necessary direction on their security roles and responsibilities, or revising its current CISPs to otherwise ensure that its IT Directors are appropriately trained on their security roles and responsibilities.

C. Clarifying who the "organization" is in CISP-002, Section 6.2, as it relates to the security training requirements stated therein.

D. Maintaining documentation that demonstrates whether sanctions/corrective actions for OIT employees and external users were enforced for security training noncompliance or whether full compliance with the most current year's training was met, and therefore, no sanctions/corrective actions were necessary.

E. Maintaining documentation that demonstrates whether sanctions/corrective actions for OIT employees and external users were enforced for Acceptable Use Policy attestation noncompliance or whether full compliance was met, and therefore, no sanctions/corrective actions were necessary.

F. Updating the OIT Human Resources' communication to OIT executive leadership, as required within the Business Operating Procedure, BOP-HR-001, to clarify whether the reported

information includes any noncompliance with the Acceptable Use Policy attestation requirements.

G. Holding OIT's IT Directors accountable by requiring documentation of follow up procedures performed with the agency or agencies each IT Director represents to ensure the agencies are applying agency-level sanctions for noncompliance with security training and Acceptable Use Policy attestations.

Response

Governor's Office of Information Technology

A. Disagree
Implementation Date: Not Applicable

The new CISP does not require role-based security training.

Auditor's Addendum

As noted in the finding, OIT's December 2024 CISP-002, which was effective and enforceable during the audit, requires OIT to develop and conduct security training and awareness programs, including role-based training for consolidated agencies. Further, NIST indicates that users with significant cybersecurity and/or privacy responsibilities require an individualized program of role-based training to ensure that their knowledge and skills are sufficient to execute the tasks required for their work. As the State's Technology Provider, OIT is ultimately responsible for ensuring users are sufficiently trained to perform their security-related roles and responsibilities.

B. Disagree
Implementation Date: Not Applicable

The new CISP does not require role-based security training.

Auditor's Addendum

As noted in the finding, OIT did not demonstrate that it had followed its December 2024 CISP-002 requiring OIT to develop and conduct security training and awareness programs, including role-based training for its IT Directors. Further, OIT did not provide documentation to demonstrate that it had provided any specific role-based training to IT Directors on their security roles and responsibilities to effectively support the agencies they represent.

C. Disagree
Implementation Date: Not Applicable

Security policies and standards are up to date with glossary definitions for key terms.

Auditor's Addendum

As noted in the finding, OIT has not defined the term "organization" in its December 2024 CISP-002. Thus, OIT has not clearly established and communicated who is responsible for providing role-based security training.

D. Disagree
Implementation Date: Not Applicable

OIT maintains documentation that demonstrates whether sanctions/corrective actions for OIT employees and OIT contractors were enforced for security training noncompliance. As for external users, OIT provides reports to Product Directors but we cannot enforce compliance at the agencies.

Auditor's Addendum

As noted in the finding, OIT did not provide documentation to demonstrate that sanctions/corrective actions for OIT employees and OIT contractors were enforced for security training noncompliance or whether full compliance with the most current year's training was met, and therefore, no sanctions/corrective actions were necessary. Further, our finding and recommendation was specific to OIT and did not extend to agency or "external" users.

E. Disagree
Implementation Date: Not Applicable

OIT maintains documentation that demonstrates that sanctions/corrective actions for OIT employees and OIT contractors were enforced for security training noncompliance. As for external users, OIT provides reports to Product Directors but we cannot enforce compliance at the agencies.

Auditor's Addendum

OIT did not provide documentation to demonstrate that sanctions/corrective actions for OIT employees and OIT contractors were enforced for Acceptable Use Policy attestation noncompliance or whether full compliance was met, and therefore, no sanctions/corrective actions were necessary. Further, our finding and recommendation was specific to OIT employees and contractors and did not extend to agency users.

F. Agree
Implementation Date: January 2026

Current communication and reporting to executive leadership does include AUP attestations, cybersecurity and ALL required Training. Business Operations Procedure (BOP-HR 001) will be modified to state that.

G. Disagree
Implementation Date: Not Applicable

OIT is now tasking ITDs with communicating non-compliance to each agency monthly. Enforcing compliance by other agencies is outside of OIT's authority.

Auditor's Addendum

As noted in the finding, OIT's Monthly Communication Email Template from OIT's Chief Customer Officer and Chief Information Security Officer to OIT's IT Directors, which was effective and enforceable during the audit, already requires that the IT Directors share, or communicate, the information related to noncompliance with mandatory training and Acceptable Use Policy attestations with the agency contact that is responsible for taking action on any noncompliance. Further, the state CISO is statutorily required to enforce CISPs, and CISP-002, IT Security and Awareness Training, Section 7.2 and CISP-018, Acceptable Use of State Data and IT Resources, Section 18 state that failure to comply with this policy may result in, as applicable, agency-level sanctions regarding state IT resources: restriction, deactivation, or suspension of the project or system.

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876