



Enterprise Information Services

EIS Should Strengthen IT Governance and Risk Oversight

October 2026

Report 2026-28



Oregon
Secretary of State

Audit Summary

Enterprise Information Services

EIS Should Strengthen IT Governance and Risk Oversight

OBJECTIVES

Our objectives were to (1) Determine whether Data Center Services has designed and implemented controls to ensure the security of systems and data it hosts or manages; (2) Determine whether Cyber Security Services has designed and implemented appropriate controls over centralized security operations across all applicable entities, including those outside Data Center Services' management; and (3) Determine if Data Center Services and Cyber Security Services provides a controlled and stable operating environment for agency enterprise applications.

SCOPE

The scope of this audit focused on assessing cybersecurity and operational controls within Enterprise Information Services (EIS), including its Data Center Services (DCS) and Cyber Security Services (CSS) programs, during 2025 and early 2026. We reviewed cybersecurity safeguards designed to protect state systems and data, detect and respond to threats, and support secure operations across enterprise infrastructure, including controls related to asset and software management, access control, system configuration, monitoring and logging, incident response, and third-party risk. We also reviewed operational processes supporting reliable and resilient technology services, including security governance, physical and environmental protections, and disaster recovery and continuity. In addition, we reviewed core processes for job scheduling and monitoring, performance and capacity management, problem management, and incident management to assess whether systems remain stable, secure, and available. We did not review all operations, such as those related to customer service.

Why this audit is important

With a biennial budget of approximately \$345 million, EIS, including DCS, invests significant public resources in enterprise technology systems that support critical government operations. Effective cybersecurity and operational controls are essential to protecting these investments and ensuring they deliver intended value.

State systems support essential services such as healthcare, public safety, and economic programs. Ensuring these systems are secure, reliable, and resilient helps protect sensitive information and ensures Oregonians can depend on government services when they need them most.

EIS operates within a complex shared-services environment where responsibilities for cybersecurity, security operations, and service delivery are distributed across multiple organizations, including programs within EIS such as DCS and CSS, as well as customer agencies. Strong governance, coordination, and consistent control implementation are critical to ensuring enterprise-wide effectiveness.

What we found

Enterprise cybersecurity controls are largely implemented, but governance and accountability gaps remain. (pg. 4)

EIS has partially to fully implemented 89% of the relevant cybersecurity safeguards aligned with the CIS Critical Security Controls®, providing an adequate cybersecurity foundation for protecting the State's enterprise technology environment. Through centralized security capabilities, EIS has established a range of controls that support threat detection, system

protection, and incident response across multiple platforms. However, EIS should further strengthen enterprise governance, accountability, and consistency of control implementation within the state's complex shared services model. Addressing the governance and accountability improvements identified in this audit will help EIS continue to mature the state's enterprise cybersecurity program. Due to the sensitive nature of these cybersecurity conditions, we presented further details of the cybersecurity findings in two confidential appendices provided directly to EIS management.

Operational controls provide a stable environment, but enterprise oversight and consistency should be improved.
(pg. 5)

EIS has implemented operational processes that provide a stable and controlled computing environment. DCS and CSS maintain structured procedures for service monitoring, incident response, and operational support across the state's diverse enterprise platforms and infrastructure. These capabilities provide an operational foundation that helps sustain system availability and enables coordinated responses when issues arise. As enterprise services and shared responsibilities continue to mature, EIS should improve enterprise-level oversight, consistency, and performance measurement. Addressing these weaknesses will enhance EIS's ability to provide enterprise assurance that operational processes are functioning consistently and support reliable service delivery across the statewide environment.

What we recommend

To improve cybersecurity, EIS should:

1. Address confidential findings included in confidential Appendix A.

To improve enterprise security management and expand oversight, we recommend EIS:

2. Update the Information Security Program Plan to explicitly document control ownership, shared responsibility models, and accountability boundaries across CSS, DCS, DAS IT, and agencies. The revised plan should include role-based responsibility matrices tied directly to control families and be formally disseminated and acknowledged by participating organizations.
3. Complete a formal, enterprise-wide risk assessment to establish a documented risk baseline and integrate the results into the statewide risk management strategy. Update the strategy to explicitly address both security and privacy risks and require periodic reassessment on a defined cadence.
4. Establish a recurring internal security control assessment program, including defined assessment plans, independence criteria, and documented results. Use assessment outcomes to inform risk management decisions.
5. Enhance the Plan of Action and Milestones (POA&M) process by implementing standardized enterprise metrics and periodic management reporting. Use aggregated POA&M data to identify trends, prioritize remediation, and support continuous improvement.

To address physical security policy and review documentation weaknesses, EIS should:

6. Develop and formally approve a stand-alone internal Physical and Environmental Protection Policy. The policy should define scope, roles, accountability, review cadence, and integration with facilities, continuity, and incident response programs.
7. Establish standardized documentation requirements for physical access reviews, including defined artifacts, retention periods, and management sign-off. Documentation should be centrally stored and periodically reviewed for completeness.

To address disaster recovery and continuity weaknesses, EIS should:

8. Establish and enforce an enterprise-wide process to define, approve, and periodically review Recovery Time Objectives and Recovery Point Objectives for all critical systems and services, ensuring alignment with business impact analyses and documented risk tolerance.

9. Standardize disaster recovery plan content, require periodic validation of completeness, and ensure all plans are centrally maintained, current, and accessible to incident responders.
10. Implement an enterprise-level Disaster Recovery (DR) testing strategy that defines minimum testing frequency, scope, documentation requirements, and remediation tracking for all critical systems.
11. Formally define DR roles and responsibilities, incorporate them into training and exercises, and ensure coverage plans exist for key recovery functions.
12. Formally incorporate network resiliency into the disaster recovery and continuity program by defining recovery objectives for critical network services, documenting network recovery procedures and dependencies within DR plans, and requiring periodic testing of network failover and recovery scenarios.

To address job scheduling and monitoring governance weaknesses, EIS should:

13. Establish an enterprise job scheduling governance framework that is aligned to best practices and integrated into operational control monitoring to ensure sustained accountability and documentation maturity. At minimum, the framework should:
 - a. Assign a formally documented and accountable owner for each critical scheduled job or job stream,
 - b. Require standardized documentation of job purpose, upstream and downstream dependencies, recovery procedures, escalation contacts, and business impact classification,
 - c. Define shared responsibility boundaries between scheduler platform teams and application owners, and
 - d. Require periodic review and validation of job documentation and ownership assignments.

To address performance and capacity management weaknesses, EIS should:

14. Establish a formal enterprise Performance and Capacity Management framework that integrates operational monitoring activities into a centralized governance structure, ensuring performance and capacity management transitions from reactive infrastructure support to proactive enterprise risk management. At a minimum, the framework should:
 - a. Define and document approved service level and performance objectives tied to business requirements,
 - b. Integrate forward-looking capacity forecasting with statewide modernization plans, cloud strategy, and vendor management,
 - c. Assign a clearly designated enterprise-level accountable owner responsible for availability and capacity governance, and
 - d. Require periodic enterprise performance reporting to executive leadership, including trend analysis and capacity risk indicators.

To address weaknesses identified with problem management, EIS should:

15. Formally institutionalize an enterprise-wide problem management framework. Specifically, management should:
 - a. Designate an accountable enterprise owner for lifecycle governance,
 - b. Establish standardized criteria for incident-to-problem escalation and risk-based prioritization,
 - c. Implement a documented and required root cause analysis methodology,
 - d. Develop a centralized Known Error Database integrated with the ticketing system,
 - e. Require formal validation of corrective actions prior to problem closure, and
 - f. Establish periodic enterprise reporting on problem trends, aging backlog, recurring root causes, and systemic risk exposure.

To address weaknesses identified with managing incidents, EIS should:

16. Establish a formal enterprise Incident Management Governance Framework. This framework should:
 - a. Define standardized enterprise-wide incident classification and prioritization criteria,
 - b. Establish clear escalation thresholds and executive notification requirements,
 - c. Assign an accountable enterprise owner for incident management effectiveness across CSS, DCS, and agencies,

- d. Require documented root cause analysis for significant incidents and centralized tracking of corrective actions,
- e. Implement enterprise-level incident metrics and dashboards (e.g., mean time to detect, contain, recover; recurrence rates; corrective action aging), and
- f. Require periodic testing of communication methods and escalation pathways.

Agency response

We made 16 recommendations to EIS in this public report and nine recommendations in confidential Appendix A. EIS agreed with all of our recommendations. The response can be found at the end of the report.

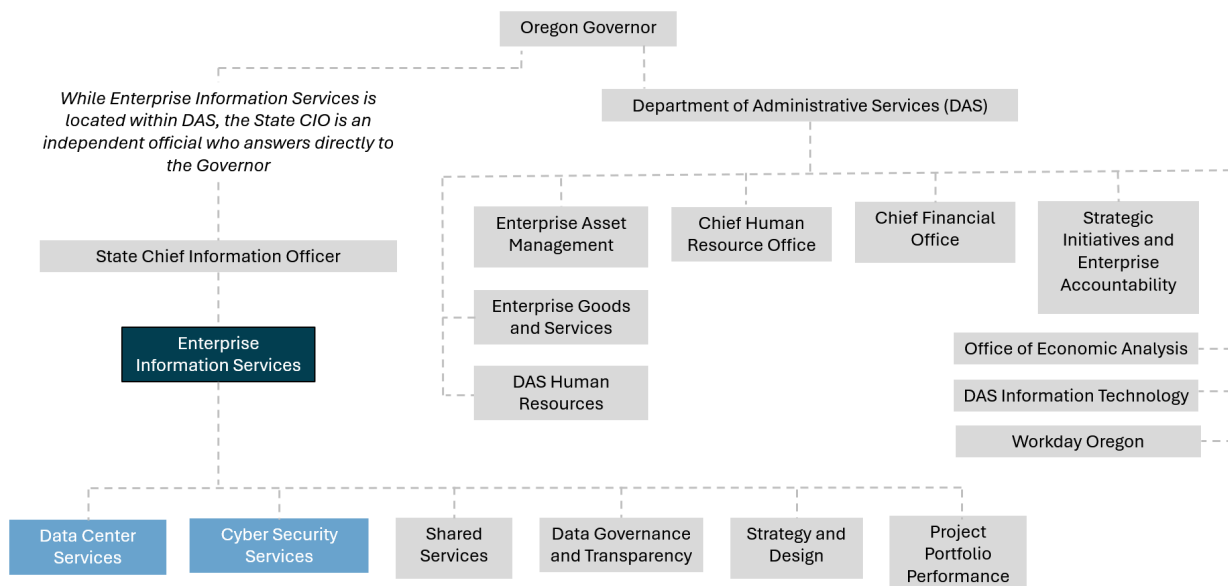
Read the full audit report at sos.oregon.gov/audits

Introduction

Enterprise Information Services (EIS) is the centralized enterprise information technology organization for the State of Oregon, operating within the Department of Administrative Services (DAS). While EIS is an organizational component of DAS, the head of EIS, the State Chief Information Officer, reports directly to the Governor. EIS is responsible for maturing statewide information technology governance and oversight, optimizing enterprise technology investments, ensuring transparency, and delivering secure and innovative information technology solutions that support the state's mission and service delivery to Oregonians. Its vision emphasizes accessible, reliable, and secure state technology systems that equitably serve the public.

EIS's mission and strategic direction are formally articulated in its Strategic Framework 2023–2026,¹ which establishes enterprise priorities, guiding principles, and measurable outcomes across technology governance, cybersecurity, cloud adoption, data governance, and legacy system modernization.

Figure 1: EIS organizational structure and leadership



Source: Created by OAD

EIS is led by the State Chief Information Officer (State CIO), supported by an executive leadership team that includes a deputy CIO, program directors, and enterprise chiefs (e.g., Chief Information Security Officer, Chief Data Officer).

EIS budgetary and investment context

As of the 2025-27 Legislatively Adopted Budget, EIS and Data Center Services (DCS) have a combined budget of approximately \$345 million and is comprised of 282 staff organized across seven primary

¹ [EIS Strategic Framework 2023-2026](#)

programs, each with distinct and interrelated responsibilities. This staffing model reflects EIS's role as both a centralized governance authority and an operational service provider for the enterprise.

EIS manages a significant statewide IT services budget funded through a combination of legislative appropriations, rate-based cost recovery, and agency service charges. Its budget supports enterprise infrastructure operations, cybersecurity services, data center facilities, staffing, and statewide governance functions. EIS also plays a central role in reviewing, prioritizing, and overseeing agency IT investments through enterprise governance processes. While individual agency systems remain agency-owned, EIS's oversight role places it at the center of statewide technology risk, cost optimization, and performance accountability.

EIS has statutory authority and oversight for IT security of state agencies

EIS derives its enterprise authority primarily through the State CIO, who is statutorily designated under ORS 276A² to provide statewide leadership, oversight, and coordination of information technology across Oregon's executive branch agencies. Through this authority, EIS sets statewide IT policies, standards, and control expectations, and provides shared services that agencies rely on for core infrastructure, security, and governance functions.

EIS functions as both:

- A governance body, establishing statewide policies, standards, and oversight mechanisms; and
- A service provider, delivering shared infrastructure, cybersecurity, and operational services to agencies.

This dual role makes EIS a critical focal point for statewide IT risk management, accountability, and consistency, particularly in areas related to cybersecurity, enterprise infrastructure, and major IT investments. With many agency applications and systems residing in the state's data center operated by DCS, and most agency information technology traffic traversing the state network, EIS is positioned to provide the enterprise-level governance, security, and operational oversight needed to support consistent, reliable technology controls across state government.

With respect to cybersecurity specifically, ORS 276A.300 provides that the State CIO has responsibility for and authority over information systems security in the executive department. This includes establishing the statewide security plan and associated standards and coordinating activities such as reviewing and verifying agency system security, monitoring state network traffic for threats, and conducting vulnerability assessments. Oregon's administrative rules further reinforce this statewide oversight structure through OAR Chapter 128,³ Division 30, though it refers to DAS generally as opposed to the role of the State CIO or EIS. In particular, OAR 128-30-0020 describes DAS's statewide information security duties, including central leadership, security assessments, statewide reporting, and "compliance and oversight," such as directing compliance reviews and taking action when agencies fail to adhere to information security practices.

² [ORS 276A](#)

³ [OAR Chapter 128](#)

State IT Security oversight exemptions

The State CIO has oversight over executive branch agencies excluding the Secretary of State, State Treasurer, and Attorney General, who have sole discretion and authority over their information systems security. These agencies are required to collaborate with the State CIO on their security planning and compatibility with the statewide security plan.

EIS's programs collectively support enterprise governance, security, infrastructure, and service delivery

While EIS's areas of responsibility cover multiple governance and service functions, our audit focused on the programs operated by DCS and CSS.

Data Center Services (DCS)

DCS delivers enterprise computing, hosting, network, and platform services, including mainframe, midrange, distributed systems, and network infrastructure. DCS operates the state's data center and maintains service catalogs aligned with customer demand, funding models, and security standards.

Cyber Security Services (CSS)

CSS centralizes enterprise cybersecurity governance, architecture, operations, and monitoring. CSS establishes statewide security policy and controls, delivers security services, and operates the Security Operations Center (SOC) providing continuous monitoring and incident response across the enterprise.

Project Portfolio Performance (P3)

Provides statewide oversight of major IT investments through the IT Governance Framework. P3 manages portfolio transparency, tiered project oversight, investment risk assessment, and alignment with enterprise strategies, policies, and statutory requirements.

Shared Services

Coordinates and delivers enterprise-wide shared capabilities, including e-government platforms, quality assurance functions, and statewide interoperability services. This program also advances shared-service delivery models to reduce duplication and improve consistency.

Strategy and Design

Leads enterprise architecture, technology standards, and strategic technology initiatives to align business needs with long-term enterprise IT strategy, including cloud, modernization, and digital transformation efforts.

Data Governance and Transparency

Oversees statewide data governance, open data standards, enterprise data strategy, and public transparency initiatives, including management of Oregon's open data and transparency platforms.

Administrative Services

Provides budget management, executive support, internal governance, and project management services.

Audit Results

Overall, Enterprise Information Services (EIS) has designed and implemented operational and security controls aligned with best practices and standards for delivering enterprise technology services to Oregon state agencies. These controls extend across cybersecurity, security management, physical security, disaster recovery, and other operational areas. Specifically, we found EIS had at least partially implemented 89% of cybersecurity safeguards we evaluated and all the operational controls we evaluated.

At the same time, EIS needs to further strengthen governance clarity, enterprise oversight, and consistency of control implementation across the complex shared-services environment in which EIS operates. Several findings identified areas to improve coordination of responsibilities, enhance enterprise-level risk monitoring, and strengthen assurance mechanisms that confirm controls are operating consistently across platforms and organizational boundaries. Addressing these weaknesses will help EIS build upon its existing foundations and continue maturing its enterprise security and operational management practices while supporting the state's broader objectives for secure, reliable, and resilient technology services.

Enterprise cybersecurity controls are largely implemented, but governance and accountability gaps remain

Centralized security functions operated by Cyber Security Services (CSS) and infrastructure services managed by Data Center Services (DCS) support threat detection, system protection, and incident response across multiple platforms. However, EIS needs to further strengthen enterprise governance, clarify accountability, and improve consistency of control implementation within the state's complex shared services model. Addressing the governance and accountability improvements identified in this audit will help EIS continue maturing the state's enterprise cybersecurity program.

The Center for Internet Security (CIS) Critical Security Controls® offers a prioritized set of cybersecurity best practices through a series of "safeguards" designed to help organizations prevent, detect, and respond to common cyber threats. These controls function as an integrated system: foundational activities such as maintaining accurate inventories of assets and software enable more advanced capabilities like centralized monitoring, intrusion detection, and coordinated incident response. The controls emphasize the importance of governance, recognizing that effective cybersecurity depends not only on technical tools, but also on clearly defined ownership, accountability, and oversight. CSS uses these controls to assess the cybersecurity posture of entities under its oversight authority.

This audit evaluated both the technical implementation of relevant CIS safeguards and governance structures that enable those safeguards to function effectively. Domains outside of the control of EIS were excluded.

At EIS, controls are implemented within a shared-services enterprise model that supports multiple state agencies, boards, and commissions across a diverse set of technology platforms. This includes cloud-hosted services, distributed server environments, network infrastructure, and specialized systems. Cybersecurity responsibilities are distributed among EIS programs, such as CSS and DCS, as well as external partners and agency IT organizations. This operating model introduces inherent complexity and risk, but also is intended to enable standardization, centralization of expertise, and economies of scale that

individual agencies, boards, or commissions would be unlikely to achieve independently. As a result, many safeguards are implemented through enterprise services rather than agency-specific controls.

Overall, EIS demonstrates alignment with the intent of the CIS Controls®; of the 399 applicable cybersecurity safeguards we evaluated, we found 355 to have been at least partially implemented. Particular areas of alignment included centralized security capabilities and enterprise service delivery. Specifically, EIS has established mature, well-documented processes for incident management and cybersecurity incident response, supported by dedicated security personnel, defined escalation paths, and service management software. Centralized security monitoring capabilities, including network-level protections, endpoint security tools, and threat intelligence integrations help detect and respond to malicious activity across the enterprise.

Platforms: The term “platform” refers to a major technology environment or service layer used to host, process, transmit, or support state systems and data. Platforms may include server environments, specialized computing environments, operating systems, cloud services, or other enterprise technologies that support agency applications and business operations. Because each platform can use different technologies, tools, administrative processes, and security capabilities, some cybersecurity and operational controls may be implemented differently across platforms.

EIS has also largely standardized security practices across platforms through enterprise configuration standards, managed security tools, and shared operational processes. Where direct technical enforcement is not feasible, due to platform constraints or legacy system limitations, EIS has implemented compensating controls, documented processes, or alternative oversight mechanisms to manage risk. EIS’s centralized security services, incident response coordination, and enterprise tools provide a foundation upon which remaining gaps can be addressed.

While EIS has broadly implemented the CIS Controls® through a combination of centralized services, platform-specific controls, and shared responsibilities with agencies and service providers, we identified areas where control design, consistency, or governance could be further strengthened. Our findings focus on conditions that limit EIS’s ability to demonstrate enterprise-wide assurance over certain CIS safeguards, particularly where responsibilities span multiple organizations or platforms.

Due to the sensitive nature of these cybersecurity conditions, we presented further details of the cybersecurity findings in two confidential appendices provided directly to EIS management. Appendix A addresses the overall cybersecurity findings and associated recommendations. Appendix B includes our evaluation of specific safeguard-level assessments of each platform. Both appendices include technical conditions and details that, if publicly disclosed, could negatively impact the state’s security posture.⁴

Operational controls provide a stable environment, but enterprise oversight and consistency should be improved

Operational controls play a critical role in maintaining stability, reliability, and resiliency of enterprise information technology services. These controls govern the day-to-day processes that ensure systems are

⁴ [ORS 192.345\(23\)](#) allows public records that may reveal security measures or potential security weaknesses to be exempt from public disclosure.

monitored, service incidents are managed, problems are analyzed, and infrastructure capacity and performance are maintained to support agency operations. At EIS, implementing effective operational controls requires coordination between DCS, CSS, and customer agencies to ensure responsibilities are clearly executed and enterprise risks are appropriately monitored. These operational processes support EIS's broader mission of delivering accessible, reliable, and secure technology services that enable state agencies to serve Oregonians.

Overall, EIS has implemented operational processes that provide a stable and controlled computing environment. We evaluated 44 operational controls and found EIS has at least partially implemented all of them. DCS and CSS maintain structured procedures for service monitoring, service incident response, and operational support across the State's diverse enterprise platforms and infrastructure. These capabilities provide an operational foundation that helps sustain system availability and enables coordinated responses when issues arise. As enterprise services and shared responsibilities continue to mature, EIS should strengthen enterprise-level oversight, consistency, and performance measurement. Addressing these weaknesses will enhance EIS's ability to ensure operational processes are functioning consistently and supporting reliable service delivery across the statewide environment.

Security management is established, but enterprise risk oversight needs further maturation

Security management is the foundational governance layer that enables an organization to establish, oversee, and continuously improve the protection of its information systems and data. Effective security management ensures that policies, roles, responsibilities, and oversight mechanisms are clearly defined and consistently applied, allowing technical and operational security controls to function as intended. In a complex, multi-agency environment, security management is especially critical. It provides the structure necessary to coordinate activities across shared services, align risk management with organizational objectives, and maintain accountability for enterprise-wide security outcomes.

Overall, EIS has established a foundation for security management through centralized governance, clearly articulated leadership roles, extensive policies and standards, and active oversight mechanisms. EIS should build upon the foundation and enhance the effectiveness and maturity of EIS's security management practices. As with many large, shared-services environments, the complexity of coordinating risk management, assessment activities, and accountability across multiple organizational boundaries introduces challenges that need continued attention.

The Information Security Program Plan does not clearly define shared control ownership, increasing the risk of accountability gaps.

While EIS maintains a documented, NIST⁵-aligned Information Security Program Plan, it does not fully reflect how security responsibilities are executed within the current shared-services model.

Specifically, the plan outlines high-level authority and oversight but does not clearly define control ownership, accountability, or execution responsibilities across CSS, DCS, and customer agencies, resulting in inconsistent interpretation of roles and expectations. This condition stems from the plan evolving incrementally alongside the transition to centralized and shared services without being comprehensively updated to align governance structures with operational realities, leaving

⁵ [NIST SP 800-53 Rev. 5](#)

accountability boundaries insufficiently defined. As a result, accountability gaps increase the risk that security controls are inconsistently implemented, monitored, or enforced across the enterprise, limiting EIS's ability to ensure effective control operation and elevating the potential for unaddressed risks.

Why This Matters: State technology services are shared across multiple teams and agencies. When the security plan does not clearly say who owns each responsibility, important security controls may fall through the cracks because everyone may think someone else is handling them.

EIS lacks a completed enterprise risk baseline, limiting its risk-informed decision-making

EIS has established a NIST-aligned risk management strategy and performs multiple risk-related activities. However, it has not completed a comprehensive enterprise-wide risk assessment to establish a current enterprise risk baseline. This has resulted in risk identification and prioritization occurring unevenly across programs and platforms, with reliance on external audits or localized tracking and limited integration of privacy risks. This is primarily due to a historical emphasis on external compliance and operational priorities rather than a recurring internal enterprise risk assessment process, and competing demands that have delayed completion of a statewide assessment. As a result, leadership lacks a complete view of enterprise risk. As such, risk treatment decisions will be reactive, inconsistently prioritized, and inefficiently resourced, limiting EIS's ability to align risk-informed decisions with statewide priorities and effectively manage emerging threats.

Independent internal control assessments are not performed at the state level, reducing proactive assurance

EIS performs security control assessments through CSS-led activities and external compliance audits. However, it does not conduct a recurring, independent internal assessment of controls at the enterprise level, and does not consistently document or consolidate assessment results across systems and services. This is driven by prioritization of external compliance requirements and operational delivery over developing an internal assessment capability, with no formally established assessment cycle or defined ownership for enterprise-wide independent validation. As a result, control weaknesses may remain undetected between audits, management may receive incomplete or delayed assurance, and control effectiveness cannot be consistently evaluated across the environment, limiting EIS's ability to proactively identify and remediate risks.

The Plan of Action and Milestone (POA&M) process is reactive and lacks enterprise performance metrics, limiting continuous improvement

While EIS maintains a documented POA&M process to track remediation activities, the process is largely reactive and driven by external audit findings, and enterprise-level performance metrics are not consistently defined or reported to monitor remediation effectiveness across agencies. This condition is driven by the POA&M process evolving primarily to support audit compliance rather than enterprise performance management, with no requirement to aggregate data for enterprise-wide analysis or trend identification. As a result, management has limited visibility into program effectiveness, recurring control weaknesses may persist without detection, and remediation efforts may not be prioritized based on risk, reducing the process's effectiveness as a governance and continuous improvement tool.

By addressing these risks, EIS can strengthen enterprise accountability, improve visibility into security risk, and support more informed, risk-based decision-making. Clarifying control ownership, establishing a statewide risk baseline, and enhancing independent assessments and POA&M processes will improve consistency, strengthen assurance, and enable more effective continuous improvement. Collectively, these actions will improve EIS's ability to manage enterprise cybersecurity risk across its shared-services environment.

Physical and environmental controls protect critical facilities, but documentation and governance should be strengthened

Physical security and environmental controls are foundational to safeguarding the confidentiality, integrity, and availability of enterprise information systems. These controls protect the physical facilities, infrastructure, and supporting utilities that house critical systems, safeguarding them from unauthorized access, damage, disruption, and environmental hazards. Physical and environmental protections are highly visible controls and serve as a critical first line of defense against events that can result in catastrophic system outages, data loss, or risks to personnel safety. In a statewide shared-services environment such as EIS, effective physical and environmental controls are essential to ensuring continuity of operations for multiple agencies and mission-critical services.

Physical security and environmental controls are implemented primarily through DCS, with coordination across facilities management, security operations, and enterprise security governance functions. The state's data center and associated facilities employ a layered physical security model, incorporating perimeter controls, restricted security zones, badge-based access systems, access control hallways, surveillance cameras, and 24/7 staffed monitoring. Environmental protections are integrated into this model through redundant power architecture, uninterruptible power supplies, backup generators, fire detection and suppression systems, and continuous monitoring of temperature, humidity, and power conditions. These controls are supported by documented procedures, staff training, and ongoing operational oversight.

Overall, EIS has implemented physical security and environmental controls. While EIS should strengthen documentation consistency and evidence retention, the overall control environment reflects a mostly implemented and well-functioning physical and environmental security program.

The findings identified in this section do not reflect a breakdown of physical security or environmental protections, nor do they indicate that EIS facilities are unsafe or inadequately protected. Rather, the findings focus on governance, documentation, and assurance-related gaps that limit management's ability to consistently demonstrate the effectiveness and sustainability of these controls over time. These include:

The absence of a standalone Physical and Environmental Protection Policy risks inconsistent implementation

While DCS addresses physical and environmental controls through a combination of general security policy, procedures, and operational practices, the organization does not maintain a standalone internal Physical and Environmental Protection Policy, resulting in fragmented documentation and the absence of a single authoritative source defining enterprise expectations. This condition is driven by physical security historically being treated as an operational or facilities-focused function rather than a core component of enterprise security governance, with responsibilities distributed across multiple groups and no single accountable policy owner. As a result, management lacks a centralized

framework to ensure consistent implementation and oversight, increasing the risk that physical and environmental controls are applied unevenly, insufficiently monitored, or deprioritized over time.

Physical access reviews lack consistent documentation, risking gaps in access oversight

While DCS personnel state they perform physical access reviews as part of ongoing operational practices, they do not consistently document or retain supporting evidence, limiting the ability to demonstrate that reviews are completed and effective across the enterprise. This condition is driven by a lack of standardized documentation requirements and evidence retention practices, with processes relying on informal or decentralized approaches rather than a defined governance framework. As a result, management has limited visibility into the consistency and completeness of access reviews, and there is an increased risk that inappropriate or outdated access may not be identified or remediated in a timely manner.

By addressing these risks, EIS can strengthen the consistency and clarity of its physical and environmental control framework across facilities. Establishing and implementing a standalone policy and improving documentation of access reviews will enhance governance, accountability, and auditability of critical security activities. These improvements will provide greater assurance that physical protections are operating as intended and consistently applied.

Disaster recovery and continuity capabilities support resilient operations, but enterprise testing and coordination need to be strengthened

Disaster recovery and continuity are critical components of operational resilience, ensuring that essential services and information systems can be restored and sustained following disruptive events. These capabilities protect the availability of systems and data in the face of incidents such as cyber events, infrastructure failures, natural disasters, or other operational disruptions. Effective disaster recovery and continuity programs integrate technical recovery capabilities with governance, planning, testing, and coordinated response to ensure that recovery activities align with business priorities and risk tolerance.

Within the State of Oregon, EIS plays a central role in providing shared infrastructure, security, and operational services to state agencies. EIS is responsible for operating and supporting critical platforms, network infrastructure, security operations, and enterprise technologies that support agency missions. As a result, disaster recovery and continuity capabilities implemented by EIS have a direct and material impact on the entire state's ability to maintain essential services during disruptive events.

EIS has implemented resilient data center operations, including redundant power, environmental controls, backup solutions, and enterprise monitoring capabilities. These foundational controls support the availability of critical systems and demonstrate an organizational commitment to operational resilience. Additionally, EIS has integrated disaster recovery considerations into broader enterprise policies and standards, aligning continuity planning with statewide IT control expectations and recognized frameworks.

While EIS has established a foundation for disaster recovery and continuity through resilient infrastructure, assignment of personnel, and enterprise-level governance, EIS should improve controls to ensure recovery capabilities are fully defined, consistently implemented, and demonstrably effective across all critical services. The findings that follow focus on improving the formalization, integration, and validation of disaster recovery and continuity practices, particularly where evolving technologies, shared-service dependencies, and increasing operational complexity introduce heightened risk.

Recovery Point Objective refers to how much data an organization can afford to lose after a system outage or disruption. For example, if a system has a one-hour Recovery Point Objective, the organization's goal is to be able to restore the system with no more than one hour of lost data.

Recovery Time Objective refers to how quickly an organization needs to restore a system or service after an outage. For example, if a system has a four-hour Recovery Time Objective, the organization's goal is to have that system back online within four hours.

Recovery objectives are not consistently defined or standardized statewide, increasing risk of misaligned restoration priorities

EIS has established high-level continuity and disaster recovery policies and performs recovery planning activities across critical platforms and environments. However, Recovery Time Objectives and Recovery Point Objectives are not consistently defined, documented, or standardized across all critical systems. We found some recovery objectives were based on informal assumptions or verbal understanding rather than approved documentation. This condition is driven by a lack of a fully institutionalized, business-driven process for defining continuity requirements, inconsistent business impact analysis activities, and the complexity of shared services ownership across EIS and customer agencies. As a result, recovery priorities may not align with actual business needs during a disruption, increasing the risk of prolonged outages, unmet service expectations, and reduced ability for management to assess whether disaster recovery capabilities are sufficient and aligned with enterprise risk tolerance.

Disaster recovery plans are incomplete and fragmented, increasing risk of confusion during incidents

Disaster recovery plans exist for many systems and services. However, their completeness, level of detail, and organization vary significantly, with documentation often fragmented across multiple repositories and in some cases supplemented by informal runbooks or institutional knowledge rather than comprehensive, approved plans. This condition is driven by disaster recovery planning evolving organically over time in response to platform-specific needs, audits, and system changes, without a centralized standard or consistent enforcement of documentation requirements. As a result, recovery efforts during a disruption may be hindered by unclear procedures, overlooked dependencies, and coordination challenges, increasing the risk of delays, errors, and extended service outages that could impact critical operations and public services.

Disaster recovery testing does not consistently validate full recovery capabilities, limiting recovery assurance

While EIS performs disaster recovery testing across multiple platforms, testing activities are not consistently conducted across all critical systems and often focus on partial or component-level recovery rather than validating full end-to-end service restoration, including data integrity and application functionality. This condition is driven by operational constraints, resource limitations, and decentralized ownership of testing responsibilities, resulting in inconsistent test scope, documentation, and follow-up on identified issues. As a result, management has limited assurance that recovery capabilities will function as intended during a disruption, and undetected weaknesses in recovery procedures, unidentified dependencies, or coordination may lead to increased downtime and operational impact during an actual event.

Disaster recovery roles and training are not formally defined, increasing execution risk

EIS relies on experienced personnel to execute disaster recovery activities; however, it does not consistently document roles and responsibilities or reinforce them through formal training, leaving many recovery procedures dependent on employee knowledge rather than clearly defined expectations. This condition is driven by a historical reliance on experienced teams and operational familiarity, with formal role definition and structured training not keeping pace with increasing complexity. As a result, recovery efforts during a disruption may be delayed or inconsistently executed, increasing the risk of confusion, duplicated efforts, or errors. It also reduces the organization's ability to respond effectively when key personnel are unavailable.

Network resiliency is not fully integrated into disaster recovery governance, increasing availability risk

While EIS has implemented network infrastructure intended to support availability, network resiliency requirements, recovery procedures, and testing are not consistently defined, documented, or validated as part of the disaster recovery program. Recovery plans assume network availability rather than treating it as a recovery dependency. This condition is driven by disaster recovery planning and testing efforts that focus primarily on systems, servers, and storage, with network recovery responsibilities treated as separate and not fully integrated into enterprise continuity governance. As a result, critical network dependencies such as connectivity, routing, security services, and access controls may not be restored in alignment with recovery objectives during a disruption, increasing the risk of delayed service restoration and prolonged outages across dependent systems and services.

Why This Matters: During a disaster, resilient networks help keep emergency communications and essential services connected. They allow agencies to share critical information, coordinate response efforts, and direct resources to the people and places that need them most. When networks fail, delays can put lives at risk.

By addressing these risks, EIS can improve the consistency and coordination of its disaster recovery and continuity capabilities across the enterprise. Standardizing recovery objectives, formalizing roles and training, and completing and aligning recovery plans will improve clarity and execution during disruptive events. Enhancing testing practices and integrating network resiliency into recovery governance will provide greater assurance that full restoration capabilities are achievable. Collectively, these improvements will further strengthen the state's ability to maintain resilient and reliable technology services during and after disruptions.

Job scheduling and monitoring processing support reliable system operations, but EIS should improve enterprise oversight and consistency

Job scheduling and monitoring are foundational operational controls that ensure automated processing activities execute reliably, completely, and as intended. In large, multi-platform environments, scheduled jobs support critical business functions such as financial processing, data synchronization, reporting, system maintenance, and inter-system integrations. Effective job scheduling and monitoring provide assurance that these automated processes run at the correct time, in the correct sequence, with appropriate dependencies enforced, and that exceptions are identified and addressed in a timely manner.

These controls are essential to maintaining the integrity, availability, and timeliness of enterprise information systems.

EIS implements job scheduling and monitoring within a mature shared services operating model that supports a diverse set of platforms and customer agencies. EIS operates centralized scheduling across its technical environments, including mainframe, distributed, and application-specific platforms, enabling consistent execution of recurring operational tasks. Scheduling tools are integrated into day-to-day operations and are supported by established teams responsible for overseeing system availability and processing cycles. This operational approach provides a baseline of centralized scheduling and monitoring for key environments, while some platform-specific practices remain distributed across domains.

Why This Matters: Many Oregon government services rely on overnight and automated processing to function properly. Effective job scheduling and monitoring help ensure unemployment benefits are paid on time, revenue systems operate reliably, and critical state services remain available. When problems are not detected quickly, delays can affect both individuals and businesses across Oregon.

While EIS has an established operational foundation for job scheduling and monitoring, effective governance requires management to consistently document, fully monitor, and demonstrably manage the controls across all platforms and workloads. As enterprise environments grow in complexity and automation becomes increasingly critical to business operations, even well-functioning processes exhibit gaps that increase operational risk if left unaddressed.

Inadequate governance, ownership, and documentation of scheduled job processing increased the risk of delayed or inaccurate processing

Scheduled job processing occurs across multiple platforms performed by teams responsible for managing enterprise infrastructure. While staff within DCS oversee the execution and monitoring of scheduled jobs, governance expectations and ownership responsibilities are not consistently defined across services and platforms. In addition, documentation describing job ownership, scheduling dependencies, and operational procedures is not always maintained in a standardized or centralized manner. This condition largely reflects the evolution of enterprise computing services over time, where automated processing activities developed within individual systems or platforms to meet specific operational needs. As infrastructure services expanded and became more interconnected, governance and documentation practices did not evolve at the same pace across all environments. When job ownership, dependencies, and recovery procedures are not clearly documented, failures or system changes may delay critical processing, disrupt downstream systems, and limit management's assurance that scheduled jobs are consistently controlled across the enterprise.

When governance expectations, ownership responsibilities, and documentation are not consistently defined, it can be more difficult to maintain clear accountability for scheduled job processing and to efficiently address operational issues when they arise. Strengthening governance structures and documentation practices will help improve transparency, support operational continuity, and reinforce the reliability of automated processing across the state's enterprise technology environment.

Performance and capacity management practices support stable system operations, but enterprise planning and oversight should be strengthened

Performance and capacity management is a foundational operational discipline to ensure information systems consistently deliver services at expected levels while maintaining sufficient resources to meet both current and anticipated demand. In large, shared service environments, effective performance and capacity management is critical to sustaining availability, supporting mission-critical workloads, and preventing service degradation as demand fluctuates. This discipline encompasses the proactive assessment, planning, monitoring, and adjustment of system resources, such as processing power, storage, network, and platform services, to align technical capabilities with business needs over time.

At EIS, performance and capacity management is implemented through a combination of enterprise infrastructure design, operational monitoring, and staff oversight across DCS and platform teams. EIS operates a resilient enterprise computing environment that includes redundant power, storage, network, and processing architectures designed to absorb fluctuations in demand and reduce the likelihood of performance-related outages. This architectural approach provides a baseline for availability and capacity, particularly for critical systems hosted within the state data center and supported platforms.

However, we noted performance and capacity management practices, though effective in day-to-day operations, are not always fully documented, standardized, or integrated with enterprise planning and demand management processes. EIS should further mature its performance and capacity management practices, reduce residual risk, and strengthen alignment with leading governance and management objectives.

Performance and capacity management procedures lack an enterprise-wide framework, increasing risk of service degradation

Within the EIS environment, performance monitoring and capacity management activities are performed across multiple platforms and operational teams within DCS. These teams use platform-specific tools and processes to monitor system performance and respond to capacity concerns as they arise. While these practices support day-to-day operational management, they are not always coordinated through a standardized enterprise-wide framework that defines consistent expectations for monitoring, reporting, and long-term capacity planning across services and platforms. This condition largely reflects the evolution of the state's shared services technology environment, where infrastructure services and monitoring practices developed independently within individual platforms or operational teams. As enterprise services expanded and became increasingly interconnected, performance and capacity management practices did not always evolve into a unified enterprise model.

Without a coordinated enterprise framework, leadership has limited visibility into performance trends and capacity risks across the broader technology environment. This can make it more difficult to identify emerging resource constraints or proactively plan for future service demand. Establishing a more consistent enterprise-wide approach to performance and capacity management will strengthen operational oversight and help ensure the reliability of the state's enterprise technology services.

Problem management processes are established, but enterprise oversight and risk-based prioritization should be strengthened

Effective problem management practices are a critical component of operational control maturity because they move an organization beyond reactive incident response toward structured analysis, root cause identification, and long-term risk reduction. While incident management focuses on restoring service as quickly as possible following a disruption, problem management is concerned with understanding why incidents occur, identifying patterns and trends, and implementing corrective actions to prevent recurrence. Effective problem management includes defined processes for problem escalation, standardized root cause analysis, maintenance of known error records, and validation of corrective actions prior to closure.

At EIS, centralized service management functions, enterprise monitoring capabilities, and established incident response processes provide an operational foundation that can support problem management. EIS operates in a complex shared-services model supporting multiple agencies, platforms, and mission-critical systems, which increases the importance of structured problem management. EIS uses operational teams and enterprise tools to identify and investigate recurring or high-impact operational issues in coordination with system owners and platform teams.

At the time of our fieldwork, EIS had previously operated without a formal problem management practice and was beginning to implement a new enterprise Problem Management Process Definition document. The June 2025 document established lifecycle activities, roles and responsibilities, prioritization, root cause analysis, known-error documentation, escalation, reporting, and closure expectations. We reviewed the design of this document but did not evaluate whether the new process had been consistently implemented or was operating effectively. Accordingly, our observations are based primarily on the operational practices in place before and during its rollout.

Problem management is not consistently risk-based or standardized, risking increased downtime for reoccurring incidents

Within the EIS environment, problem management activities occur across multiple operational teams responsible for maintaining enterprise infrastructure and services. While operational teams within DCS and CSS investigate incidents and address operational issues as they arise, problem management practices were not yet consistently governed or demonstrated across services and platforms. The preexisting approach was primarily reactive and did not consistently require or demonstrate documented root-cause analysis and broader evaluation of risks contributing to recurring incidents. This condition appears driven in part by the operational need to prioritize service restoration during incidents, without a consistently demonstrated follow-on process for enterprise problem analysis. As a result, management lacked assurance that problem management practices were applied consistently across platforms, services, and responsible teams.

When problem management processes are not consistently risk-based or standardized, systemic issues may be more difficult to identify and address over time. This increases the likelihood that similar operational problems may re-occur across services or platforms. Strengthening guidance and standardization for problem management will help EIS more effectively identify root causes, prioritize high-risk issues, and reduce the likelihood of recurring incidents across the state's enterprise technology environment.

Incident management processes support timely responses to operational events, but enterprise governance and performance measurement should be strengthened

Effective incident management is a foundational operational control that enables an organization to detect, respond to, recover from, and learn from unplanned disruptions affecting information systems and services. This section focuses on service incident management, which is separate from security incident management, which is covered separately in this report. Service incident management covers the end-to-end processes used to identify disruptions to IT activities, assess their impact, coordinate response activities, communicate with stakeholders, restore services, and capture lessons learned. Strong incident management practices are essential not only for minimizing service disruptions, but also for protecting the confidentiality, integrity, and availability of information assets.

At EIS, incident management is implemented through a combination of centralized and distributed processes. Detection and response activities are supported by enterprise monitoring capabilities, operational service desks, and security-focused functions that collectively provide visibility into service disruptions, recognizing that service disruptions may stem from operational issues or from security events. Incidents are logged, tracked, and resolved using formal ticketing and workflow tools, with defined roles for operational teams, escalation paths to management, and coordination across DCS, CSS, and affected customer agencies as needed based on the type of incident.

The following finding identifies where EIS's incident management practices do not fully align with best practices, particularly in areas related to governance, consistency, and enterprise oversight. Addressing this issue will strengthen management's ability to measure performance, maintain visibility into incident trends, and ensure incident management operates as a consistently governed and enterprise-wide process.

Incident governance is not consistently standardized or measured, increasing risk of delayed escalation and repeat events

Within the EIS environment, incident response activities are carried out across multiple teams responsible for maintaining enterprise infrastructure and services. While staff within DCS and CSS respond to incidents and coordinate restoration activities, incident governance practices are not always consistently standardized across services or platforms. In addition, enterprise performance metrics that measure incident response effectiveness, escalation timeliness, or recurring operational events are not consistently used to evaluate incident management performance. This condition largely reflects the operational nature of responding to incidents in a complex shared-services environment where teams must focus on quickly restoring services and maintaining system availability. As a result, incident management practices vary depending on the platform, service, or team responsible for responding to the event.

Without consistent governance practices and performance measurement, leadership lacks a consolidated view of how effectively incidents are managed across operational and security functions. This will make it more difficult to identify patterns of recurring incidents, evaluate escalation practices, or implement improvements to incident response processes. Strengthening incident governance and incorporating enterprise performance metrics will help EIS improve the reliability and resilience of the state's enterprise technology services.

Recommendations

To improve cybersecurity, EIS should:

1. Address confidential findings included in the confidential Appendix A.

To improve enterprise security management and expand oversight, we recommend EIS:

2. Update the Information Security Program Plan to explicitly document control ownership, shared responsibility models, and accountability boundaries across CSS, DCS, DAS IT, and agencies. The revised plan should include role-based responsibility matrices tied directly to control families and be formally disseminated and acknowledged by participating organizations.
3. Complete a formal, enterprise-wide risk assessment to establish a documented risk baseline and integrate the results into the statewide risk management strategy. Update the strategy to explicitly address both security and privacy risks and require periodic reassessment on a defined cadence.
4. Establish a recurring internal security control assessment program, including defined assessment plans, independence criteria, and documented results. Use assessment outcomes to inform risk management decisions.
5. Enhance the Plan of Action and Milestones (POA&M) process by implementing standardized enterprise metrics and periodic management reporting. Use aggregated POA&M data to identify trends, prioritize remediation, and support continuous improvement.

To address physical security policy and review documentation weaknesses, EIS should:

6. Develop and formally approve a stand-alone internal Physical and Environmental Protection Policy. The policy should define scope, roles, accountability, review cadence, and integration with facilities, continuity, and incident response programs.
7. Establish standardized documentation requirements for physical access reviews, including defined artifacts, retention periods, and management sign-off. Documentation should be centrally stored and periodically reviewed for completeness.

To address disaster recovery and continuity weaknesses, EIS should:

8. Establish and enforce an enterprise-wide process to define, approve, and periodically review Recovery Time Objectives and Recovery Point Objectives for all critical systems and services, ensuring alignment with business impact analyses and documented risk tolerance.
9. Standardize disaster recovery plan content, require periodic validation of completeness, and ensure all plans are centrally maintained, current, and accessible to incident responders.
10. Implement an enterprise-level Disaster Recovery (DR) testing strategy that defines minimum testing frequency, scope, documentation requirements, and remediation tracking for all critical systems.
11. Formally define DR roles and responsibilities, incorporate them into training and exercises, and ensure coverage plans exist for key recovery functions.
12. Formally incorporate network resiliency into the disaster recovery and continuity program by defining recovery objectives for critical network services, documenting network recovery procedures and dependencies within DR plans, and requiring periodic testing of network failover and recovery scenarios.

Recommendations

To address job scheduling and monitoring governance weaknesses, EIS should:

- 13.** Establish an enterprise job scheduling governance framework that is aligned to best practices and integrated into operational control monitoring to ensure sustained accountability and documentation maturity. At minimum, the framework should:
- a. Assign a formally documented and accountable owner for each critical scheduled job or job stream,
 - b. Require standardized documentation of job purpose, upstream and downstream dependencies, recovery procedures, escalation contacts, and business impact classification,
 - c. Define shared responsibility boundaries between scheduler platform teams and application owners, and
 - d. Require periodic review and validation of job documentation and ownership assignments.

To address performance and capacity management weaknesses, EIS should:

- 14.** Establish a formal enterprise Performance and Capacity Management framework that integrates operational monitoring activities into a centralized governance structure, ensuring performance and capacity management transitions from reactive infrastructure support to proactive enterprise risk management. At a minimum, the framework should:
- a. Define and document approved service level and performance objectives tied to business requirements,
 - b. Integrate forward-looking capacity forecasting with statewide modernization plans, cloud strategy, and vendor management,
 - c. Assign a clearly designated enterprise-level accountable owner responsible for availability and capacity governance, and
 - d. Require periodic enterprise performance reporting to executive leadership, including trend analysis and capacity risk indicators.

To address weaknesses identified with problem management, EIS should:

- 15.** Formally institutionalize an enterprise-wide problem management framework. Specifically, management should:
- a. Designate an accountable enterprise owner for lifecycle governance,
 - b. Establish standardized criteria for incident-to-problem escalation and risk-based prioritization,
 - c. Implement a documented and required root cause analysis methodology,
 - d. Develop a centralized Known Error Database integrated with the ticketing system,
 - e. Require formal validation of corrective actions prior to problem closure, and
 - f. Establish periodic enterprise reporting on problem trends, aging backlog, recurring root causes, and systemic risk exposure.

To address weaknesses identified with managing incidents, EIS should:

- 16.** Establish a formal enterprise Incident Management Governance Framework. This framework should:
- a. Define standardized enterprise-wide incident classification and prioritization criteria,
 - b. Establish clear escalation thresholds and executive notification requirements,
 - c. Assign an accountable enterprise owner for incident management effectiveness across CSS, DCS, and agencies,

Recommendations

- d. Require documented root cause analysis for significant incidents and centralized tracking of corrective actions,
- e. Implement enterprise-level incident metrics and dashboards (e.g., mean time to detect, contain, recover; recurrence rates; corrective action aging), and
- f. Require periodic testing of communication methods and escalation pathways.

Objective, Scope, and Methodology

OBJECTIVES

1. Determine whether Data Center Services has designed and implemented controls to ensure the security of systems and data it hosts or manages.
2. Determine whether Cyber Security Services has designed and implemented appropriate controls over centralized security operations across all applicable entities, including those outside Data Center Services' management.
3. Determine if Data Center Services and Cyber Security Services provides a controlled and stable operating environment for agency enterprise applications.

SCOPE

The scope of this audit focused on assessing cybersecurity and operational controls within Enterprise Information Services (EIS), including Data Center Services (DCS) and Cyber Security Services (CSS) programs, during 2025 and early 2026. We reviewed cybersecurity safeguards designed to protect state systems and data, detect and respond to threats, and support secure operations across enterprise infrastructure, including controls related to asset and software management, access control, system configuration, monitoring and logging, incident response, and third-party risk. We also reviewed operational processes supporting reliable and resilient technology services, including security governance, physical and environmental protections, and disaster recovery and continuity. In addition, we reviewed core processes for job scheduling and monitoring, performance and capacity management, problem management, and incident management to assess whether systems remain stable, secure, and available. We did not review all operations, such as those related to customer service.

METHODOLOGY

To address our audit objectives, we:

Reviewed:

- Governing policies and procedures;
- External CJIS reviews;
- Statewide IT Security Plans;
- Disaster Recovery Plans;
- Continuity of Operations Plan;
- Hardware and software inventory lists;
- User account lists and forms;
- Data backup records;
- Third-party contracts; and
- Network diagrams.

Observed:

- Physical and environmental controls;

- Security and event management dashboards;
- Asset inventory processes and data;
- Vulnerability scans and dashboards;
- Antimalware scans;
- Patch management dashboards; and
- Incident response tracking and metrics.

Interviewed:

- EIS Leadership;
- CSS Security Governance Team;
- CSS Security Operations Team;
- DCS Director;
- DCS Technical Teams; and
- EIS Compliance Program Manager.

We used recognized cybersecurity, security management, and IT governance frameworks as criteria for each major audit area. For cybersecurity, we used the CIS Critical Security Controls® version 8.1 and Statewide IT Security Standards to assess whether key safeguards were in place to protect systems and data. The CIS Controls® are organized into 18 control domains and use Implementation Groups to tailor safeguards based on an organization's resources, risk profile, and cybersecurity maturity. IG1 represents foundational cyber hygiene for smaller organizations with limited cybersecurity expertise; IG2 builds on IG1 for organizations with dedicated IT staff, more complex operations, and sensitive information; and IG3 includes all IG1 and IG2 safeguards and applies to organizations with specialized cybersecurity expertise, heightened availability and data protection needs, and exposure to more sophisticated threats. This audit includes cybersecurity controls applicable to IG3 organizations. This audit did not include all 18 control domains or all safeguards; the domain areas and individual safeguards not under the control of EIS were excluded from the CIS control set.

For security management, we used NIST SP 800-53 Revision 5 to assess enterprise governance, risk management, accountability, and security oversight. For physical security and environmental controls, we used NIST SP 800-53 Revision 5 to assess controls designed to protect facilities, systems, and supporting infrastructure. For job scheduling and monitoring, we used COBIT 2019 DSS01 Managed Operations to assess whether operational activities were controlled, monitored, and supported by defined responsibilities. For performance and capacity management, we used COBIT 2019 BAI04 Managed Availability and Capacity to assess whether EIS monitored performance, planned capacity, and supported service availability. For incident management, we used COBIT 2019 DSS02 Manage Service Requests and Incidents to assess whether incidents were identified, prioritized, escalated, resolved, and tracked. For problem management, we used COBIT 2019 DSS03 Managed Problems to assess whether recurring issues were analyzed, documented, and addressed to reduce future disruptions. For disaster recovery, we used COBIT 2019 DSS04 Managed Continuity to assess whether continuity and recovery processes supported timely restoration of critical services.

For all data provided, we assessed the reliability of data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

We considered the risks posed by publicly releasing any information related to security findings. We balanced the need for stakeholders, such as the Legislature, to be informed of critical or systemic IT security issues affecting the state against the need to protect the agency from additional threats. In accordance with ORS 192.345(23) and Generally Accepted Government Auditing Standards, we removed details of the security weaknesses from the report and provided agency management with two confidential appendices with additional detail and context. The confidential appendices provide most details related to objectives 1 and 2, while this public report addresses overall conclusions for objectives 1 and 2 and details for objective 3.

INTERNAL CONTROL REVIEW

We determined the following internal controls were relevant to our audit objectives and considered:

- **Control Environment**
 - We considered whether EIS established and maintained a control environment that demonstrates a commitment to integrity, ethical values, and accountability, including clearly defined roles and responsibilities across CSS, DCS, and agency stakeholders, based on our review of governance structures, policies, and organizational responsibilities.
 - We considered whether oversight structures, including executive leadership and centralized security governance functions, provided appropriate direction and accountability for cybersecurity and operational controls, based on interviews with management and review of governance documentation.
- **Risk Assessment**
 - We considered whether EIS identified, analyzed, and responded to risks, including cybersecurity threats and operational risks, based on our assessment of risk management processes, vulnerability management activities, and supporting documentation.
 - We considered whether EIS evaluated the impact of significant changes in systems, technologies, and the shared-services environment on its control environment, based on interviews, documentation review, and analysis of system implementations and operational processes.
- **Control Activities**
 - We considered whether EIS designed and implemented control activities, including technical and operational safeguards, to mitigate identified risks, based on testing of cybersecurity controls aligned with the CIS Controls® and review of operational processes across platforms.
 - We considered whether control activities were supported by formal policies, procedures, and standardized practices, and consistently implemented across environments, based on document review, walkthroughs, and testing of control execution.
 - We considered whether control activities included preventive and detective measures, such as access controls, system configurations, monitoring, and incident response processes, based on analysis of system configurations, security tools, and incident management practices.
- **Information and Communication**
 - We considered whether EIS used relevant, reliable, and timely information to support internal control operations, including monitoring, incident response, and decision-making, based on review of system-generated reports, dashboards, and supporting documentation.
- **Monitoring Activities**
 - We considered whether EIS performed ongoing monitoring activities, including system monitoring, incident tracking, and performance management, to evaluate the effectiveness of internal controls, based on review of monitoring tools, logs, and operational processes.

- We considered whether EIS conducted periodic evaluations, such as security assessments and audits, to assess control effectiveness and identify deficiencies, based on review of assessment practices and supporting documentation.
- We considered whether identified control deficiencies were tracked and remediated in a timely manner, based on evaluation of remediation processes, including plans of action and milestone tracking, and follow-up procedures.

Deficiencies with these internal controls were documented in the results section of this report.

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.

We sincerely appreciate the courtesy and cooperation extended by officials and employees of EIS during the course of this audit.

Audit team

Dawn Marquardt, JD, Deputy Director for Performance & IT Audits (Interim Audit Manager)

Erika Ungern, CISA, CISSP, Audit Manager

Matthew Owens, MBA, CISA, CISSP, Principal Auditor

Krystine McCants, M.Econ, CIA, Principal Auditor

Sheila Faulkner, Senior Auditor

Emily Alexander, Senior Auditor

ABOUT THE SECRETARY OF STATE AUDITS DIVISION

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The Secretary of State has constitutional authority to audit all state officers, agencies, boards, and commissions.

Appendix A: Cybersecurity Findings

This appendix is confidential and was separately shared with EIS.

Appendix B: CIS Safeguard Implementation Status

This appendix is confidential and was separately shared with EIS.



Oregon

Tina Kotek, Governor

Enterprise Information Services

State Chief Information Officer

550 Airport Road SE, Suite C

Salem, OR 97301

503-378-3175

October 7, 2026

Steve Bergmann, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 180
Salem, OR 97310

Dear Mr. Bergmann,

This letter provides a written response to the Audits Division's final draft audit report titled, "EIS Should Strengthen IT Governance and Risk Oversight."

Enterprise Information Services thanks the Secretary of State for performing this audit and appreciates the opportunity to respond to the audit and to provide clarification regarding the steps being taken to address the recommendations. The organization's response reflects its commitment to strengthening IT governance, improving risk oversight, and ensuring that corrective measures are appropriately documented and sustained.

Below is our detailed response to each recommendation in the audit.

RECOMMENDATION 1		
Address confidential findings included in the confidential Appendix A.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	12/31/2027	Ben Gherezgiher 971-388-9975

Narrative for Recommendation 1

EIS responded separately to all findings and recommendations identified in confidential Appendix A. The timelines and steps for remediation and corrective actions are detailed in that response.

RECOMMENDATION 2
Update the Information Security Program Plan to explicitly document control ownership, shared responsibility models, and accountability boundaries across CSS, DCS, DAS IT, and agencies. The revised plan should include role-based responsibility matrices tied directly to control families and be formally disseminated and acknowledged by participating organizations.

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	06/30/2027	Ben Gherezgiher 971-388-9975

Narrative for Recommendation 2

EIS will update the Information Security Program Plan to explicitly define control ownership, governance boundaries, and shared responsibility models across CSS, DCS, DAS IT, and partner agencies. To operationalize these accountability boundaries, CSS will lead the development of a comprehensive role-based responsibility matrix (RACI) directly mapped to foundational security control families. Once finalized, the revised plan will be formally disseminated to participating organizations, and a tracking process will be established to collect signed executive acknowledgments, ensuring state-level alignment and operational compliance.

RECOMMENDATION 3		
Complete a formal, enterprise-wide risk assessment to establish a documented risk baseline and integrate the results into the statewide risk management strategy. Update the strategy to explicitly address both security and privacy risks and require periodic reassessment on a defined cadence.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	09/30/2027	Ben Gherezgiher 971-388-9975

Narrative for Recommendation 3

EIS will initiate a formal, enterprise-wide security and privacy risk assessment to establish a comprehensive risk baseline across state infrastructure. CSS will lead this effort, incorporating the assessment results into a revised statewide risk management strategy that explicitly addresses both security and privacy risk vectors and mandates a periodic reassessment cadence. Once finalized, the updated strategy and risk baseline will be formally documented, approved by leadership, and integrated into ongoing enterprise governance frameworks.

RECOMMENDATION 4		
Establish a recurring internal security control assessment program, including defined assessment plans, independence criteria, and documented results. Use assessment outcomes to inform risk management decisions.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	06/30/2027	Ben Gherezgiher 971-388-9975

Narrative for Recommendation 4

EIS has a current CIS Controls Based Assessment Program. In addition to the existing program, EIS will enhance the program with a formal, recurring internal security control assessment program managed by CSS. This program will incorporate standardized assessment plans, explicit independent criteria for assessors, and mandatory documentation requirements for all evaluation outcomes. To ensure continuous risk alignment, CSS will integrate assessment findings directly into enterprise risk management decision-making processes, remediation tracking, and leadership reporting.

RECOMMENDATION 5		
Enhance the Plan of Action and Milestones (POA&M) process by implementing standardized enterprise metrics and periodic management reporting. Use aggregated POA&M data to identify trends, prioritize remediation, and support continuous improvement.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	09/30/2027	Ben Gherezgiher 971-388-9975

Narrative for Recommendation 5

EIS has already established a cybersecurity assessment program that is required by state statute. We will enhance components of the program as recommended. The program will incorporate standardized assessment plans, explicit independence criteria for assessors, and mandatory documentation requirements for all evaluation outcomes. To ensure continuous risk alignment, CSS will integrate assessment findings directly into enterprise risk management decision-making processes, remediation tracking, and leadership reporting.

To address physical security policy and review documentation weaknesses, EIS should:

RECOMMENDATION 6		
Develop and formally approve a stand-alone internal Physical and Environmental Protection Policy. The policy should define scope, roles, accountability, review cadence, and integration with facilities, continuity, and incident response programs.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	06/30/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 6

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

EIS agrees that physical and environmental protection requirements should be formally documented within an approved policy framework that clearly defines scope, roles, responsibilities, accountability, and review requirements.

EIS will evaluate existing physical security, facilities, continuity, emergency response, and related policies and procedures to identify current controls and gaps. Based on that assessment, EIS will establish and formally approve a Physical and Environmental Protection Policy or equivalent governance document that defines organizational responsibilities, integration points, approval authority, and a recurring review cadence.

RECOMMENDATION 7		
Establish standardized documentation requirements for physical access reviews, including defined artifacts, retention periods, and management sign-off. Documentation should be centrally stored and periodically reviewed for completeness.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	06/30/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 7

EIS agrees that physical access reviews should follow consistent documentation, approval, retention, and evidence-management requirements.

EIS will establish standardized requirements for documenting physical access reviews, including the required evidence/artifacts, reviewer and management approval, exception handling, retention requirements, review frequency, and centralized storage location. Existing access-review practices will be evaluated against the established standard to identify any required improvements.

To address disaster recovery and continuity weaknesses, EIS should:

RECOMMENDATION 8		
Establish and enforce an enterprise-wide process to define, approve, and periodically review Recovery Time Objectives and Recovery Point Objectives for all critical systems and services, ensuring alignment with business impact analyses and documented risk tolerance.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	10/1/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 8

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

EIS will design, implement, and enforce a centralized enterprise policy requiring all critical systems to have formal RTO and RPO definitions. Recovery targets will be derived directly from a comprehensive Business Impact Analysis. Executive leadership and business owners formally sign off on the established targets to ensure they match documented risk tolerance. A recurring schedule (at least annually or upon significant infrastructure change) will be implemented to review, update, and re-approve objectives.

RECOMMENDATION 9		
Standardize disaster recovery plan content, require periodic validation of completeness, and ensure all plans are centrally maintained, current, and accessible to incident responders.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	12/31/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 9

EIS agrees to standardize disaster recovery planning across EIS by establishing a consistent framework and template based on industry best practices. The effort will include executive sponsorship and cross-functional participation from applicable service areas and programs to ensure dependencies and recovery requirements are appropriately represented. Plans will be developed and improved through a phased approach, aligned with the RSI initiative where appropriate, and incorporated into the broader Business Continuity Plan. A recurring review and validation process will be established to ensure plans remain complete, accurate, and current. All approved disaster recovery plans will be maintained in a centralized, secure repository with defined ownership, access controls, naming conventions, and version management to ensure they are readily accessible to authorized incident responders. Governance and decision-making responsibilities will also be established to provide ongoing oversight and accountability.

RECOMMENDATION 10		
Implement an enterprise-level Disaster Recovery (DR) testing strategy that defines minimum testing frequency, scope, documentation requirements, and remediation tracking for all critical systems.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	10/1/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 10

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

EIS agrees to maintain and enhance an enterprise-level Disaster Recovery (DR) testing strategy that establishes minimum testing frequency, defines testing scope for critical systems, standardizes documentation and reporting requirements, and provides a consistent process for tracking remediation activities. The strategy will incorporate enterprise-wide exercises and service-area testing to validate recovery capabilities, identify gaps, and evaluate changes to systems and infrastructure. Test objectives, results, lessons learned, recovery procedures, and identified deficiencies will be documented through established EIS processes, with appropriate ownership and follow-up for corrective actions. Testing outcomes will be used to strengthen recovery procedures, improve system resiliency, and support continuous improvement of EIS disaster recovery capabilities.

RECOMMENDATION 11 Formally define DR roles and responsibilities, incorporate them into training and exercises, and ensure coverage plans exist for key recovery functions.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	12/31/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 11

EIS agrees to maintain and enhance clearly defined disaster recovery roles, responsibilities, and coverage across EIS, including designated primary and backup personnel for critical recovery functions. Incorporate these responsibilities into the DR Plan and establish ongoing cross-training, team coordination, and reporting to strengthen organizational readiness. Develop a standardized training and exercise program that includes applicable ICS, position-specific, and ITIL training, while expanding exercises to validate both primary and alternate recovery operations. Business Impact Analyses (BIA) and Business Process Analyses (BPA) will be regularly reviewed and updated to identify critical business functions, dependencies, recovery requirements, and staffing needs, ensuring appropriate coverage and continuity during a disruption.

RECOMMENDATION 12 Formally incorporate network resiliency into the disaster recovery and continuity program by defining recovery objectives for critical network services, documenting network recovery procedures and dependencies within DR plans, and requiring periodic testing of network failover and recovery scenarios.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	12/31/2027	Faheem Quadri

		971-718-6769
--	--	--------------

Narrative for Recommendation 12

EIS agrees to formally incorporate network resiliency into the EIS disaster recovery and continuity program, with Resilient Site Implementation (RSI) Phase II serving as the primary initiative to develop and advance the technical capabilities needed to improve network resiliency, failover, and recovery. As these capabilities are implemented, the DR program will incorporate them into recovery objectives for critical network services, document network recovery procedures and dependencies within DR plans, and establish periodic testing of network failover and recovery scenarios. Testing results and lessons learned will be used to validate recovery capabilities, identify gaps, and continuously improve plans and procedures. These capabilities will continue to mature through RSI Phase II and other resiliency efforts, with advancements progressively incorporated into EIS disaster recovery planning, testing, and operational practices.

To address job scheduling and monitoring governance weaknesses, EIS should:

RECOMMENDATION 13 Establish an enterprise job scheduling governance framework that is aligned to best practices and integrated into operational control monitoring to ensure sustained accountability and documentation maturity. At minimum, the framework should: - Assign a formally documented and accountable owner for each critical scheduled job or job stream, - Require standardized documentation of job purpose, upstream and downstream dependencies, recovery procedures, escalation contacts, and business impact classification, - Define shared responsibility boundaries between scheduler platform teams and application owners, and - Require periodic review and validation of job documentation and ownership assignments.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	12/31/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 13

EIS agrees to enhance an enterprise job scheduling governance framework aligned with applicable best practices and integrated with operational monitoring and control processes. The framework will establish consistent requirements for ownership, documentation, responsibilities, and ongoing validation of critical scheduled jobs and job streams.

- EIS will maintain and enhance formally documented ownership for each critical scheduled job or job stream. Accountable applications or business owners and

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

appropriate operational support responsibilities will be identified and maintained as part of the governance process.

- b. EIS will maintain and enhance standards that will include, as applicable, job purpose, schedule, dependencies, business impact/criticality, recovery and restart procedures, escalation paths, support contacts, and applicable monitoring requirements. Existing documentation will be evaluated against the standard before determining remediation requirements.
- c. EIS will maintain and enhance a responsibility model that distinguishes platform administration and monitoring from application/job ownership, including responsibility for job configuration, dependencies, recovery instructions, escalation, and business-impact decisions.
- d. EIS will maintain and enhance a defined review cadence for critical jobs and require validation following significant application, infrastructure, ownership, or scheduling changes. The governance framework will identify who performs the review and how completion is documented.

To address performance and capacity management weaknesses, EIS should:

RECOMMENDATION 14

Establish a formal enterprise Performance and Capacity Management framework that integrates operational monitoring activities into a centralized governance structure, ensuring performance and capacity management transitions from reactive infrastructure support to proactive enterprise risk management. At a minimum, the framework should:

- a. Define and document approved service level and performance objectives tied to business requirements,
- b. Integrate forward-looking capacity forecasting with statewide modernization plans, cloud strategy, and vendor management,
- c. Assign a clearly designated enterprise-level accountable owner responsible for availability and capacity governance, and
- d. Require periodic enterprise performance reporting to executive leadership, including trend analysis and capacity risk indicators.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	06/30/2028	Faheem Quadri 971-718-6769

Narrative for Recommendation 14

Management Response – Recommendation 14

EIS agrees with the recommendation to establish a formal enterprise Performance and Capacity Management framework. Current performance and capacity activities exist across infrastructure, cloud, network, storage, compute, and vendor-supported services; however, these practices are not yet consistently integrated into a single enterprise governance framework. EIS will formalize

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

an enterprise approach that connects operational monitoring, service performance, capacity forecasting, modernization planning, cloud strategy, vendor management, and executive risk reporting.

The framework will include the following:

14.a – EIS will define and document approved service-level, availability, performance, and capacity objectives for critical enterprise services. Objectives will be aligned with business requirements, service commitments, technical architecture, and applicable customer or vendor agreements. Where formal targets already exist, EIS will evaluate and incorporate them into the enterprise framework.

14.b – EIS will establish a forward-looking capacity planning process that considers historical utilization, projected growth, modernization initiatives, cloud adoption, lifecycle requirements, disaster recovery and resiliency needs, and vendor capacity commitments. Capacity planning will be incorporated into relevant statewide technology planning and investment decisions so emerging constraints can be identified before they become operational issues.

14.c – EIS leadership will designate an accountable enterprise owner for Performance, Availability, and Capacity Management. The accountable owner will establish governance standards, coordinate responsibilities across service towers, define reporting expectations, and ensure risks requiring enterprise action are escalated appropriately. Individual technology teams will continue to retain responsibility for day-to-day monitoring and management of their respective services.

14.d – EIS will develop periodic enterprise reporting for executive leadership that provides visibility into service performance, availability, utilization trends, capacity forecasts, significant constraints, vendor dependencies, and emerging capacity risks. Reporting will emphasize trend analysis and actionable risk indicators rather than relying solely on point-in-time operational metrics.

To address weaknesses identified with problem management, EIS should:

RECOMMENDATION 15

Formally institutionalize an enterprise-wide problem management framework. Specifically, management should:

- a. Designate an accountable enterprise owner for lifecycle governance,
- b. Establish standardized criteria for incident-to-problem escalation and risk-based prioritization,
- c. Implement a documented and required root cause analysis methodology,
- d. Develop a centralized Known Error Database integrated with the ticketing system,
- e. Require formal validation of corrective actions prior to problem closure, and
- f. Establish periodic enterprise reporting on problem trends, aging backlog, recurring root causes, and systemic risk exposure.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	07/31/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 15

EIS agrees to formally institutionalize and continue maturing an enterprise-wide Problem Management framework. EIS has an established Problem Management Process Definition Document that defines key roles, processes, governance expectations, escalation practices, and reporting requirements since the audit. This existing framework, along with current ITSM capabilities, will serve as the foundation for strengthening consistency, accountability, documentation, and enterprise oversight of Problem Management.

15.a - EIS has defined Problem Management roles, including an accountable Process Owner responsible for governance and effectiveness of the process across the organization. EIS will continue to formalize this accountability to ensure consistent lifecycle governance and enterprise oversight.

15.b - EIS has established Problem Management processes that include problem identification, categorization, prioritization, and escalation. These practices will continue to be standardized and matured to provide consistent criteria for determining when incidents should transition to Problem Management and how problems are prioritized based on impact, urgency, recurrence, and organizational risk.

15.c - EIS will formalize consistent Root Cause Analysis (RCA) requirements for applicable problems. The framework will support recognized RCA techniques while focusing on identifying underlying causes, documenting findings, determining corrective actions, and preventing recurrence.

Commonly used RCA techniques within ITIL environments include:

- Five Whys
- Ishikawa (Fishbone) diagrams
- Fault tree analysis
- Kepner Tregoe
- Brainstorming and affinity grouping
- Pareto analysis

15.d - EIS currently maintains Known Error records within the ITSM Problem Management environment and links them to applicable tickets. This capability will continue to mature toward a centralized Known Error Database that provides consistent documentation, visibility, and integration with Incident and Problem Management processes.

15.e - EIS will maintain requirements for validating corrective actions before problems and associated Known Errors are formally closed. Existing change management and verification

processes will be leveraged to confirm corrective actions have been successfully implemented and that the underlying issue has been appropriately addressed.

15.f - EIS will continue to mature enterprise Problem Management reporting to provide leadership with visibility into problem trends, aging and backlog, recurring issues and root causes, corrective action progress, and systemic risks. Existing ITSM and reporting capabilities will be leveraged and enhanced to support ongoing governance, management oversight, and continuous improvement.

RECOMMENDATION 16

Establish a formal enterprise Incident Management Governance Framework. This framework should:

- a. Define standardized enterprise-wide incident classification and prioritization criteria,
- b. Establish clear escalation thresholds and executive notification requirements,
- c. Assign an accountable enterprise owner for incident management effectiveness across CSS, DCS, and agencies,
- d. Require documented root cause analysis for significant incidents and centralized tracking of corrective actions,
- e. Implement enterprise-level incident metrics and dashboards (e.g., mean time to detect, contain, recover; recurrence rates; corrective action aging), and
- f. Require periodic testing of communication methods and escalation pathways.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	07/31/2027	Faheem Quadri 971-718-6769

Narrative for Recommendation 16

EIS agrees to formalize and standardize incident management governance across CSS, DCS, and supported agencies. Existing incident management practices, escalation procedures, communication processes, and operational response activities provide a foundation; however, they are not yet consistently defined or governed as a single enterprise framework. EIS will develop an enterprise Incident Management Governance Framework that establishes common expectations for classification, prioritization, escalation, executive notification, ownership, root cause analysis, corrective action tracking, performance measurement, and periodic testing of communication and escalation processes.

16.a – EIS will establish standardized enterprise-wide incident classification and prioritization criteria to ensure incidents are evaluated consistently based on business impact, service impact, urgency, scope, customer impact, security considerations, and operational risk. Existing severity

and priority practices will be reviewed and aligned into a common enterprise model with clearly documented definitions, decision criteria, and responsibilities.

16.b – EIS will establish clearly defined escalation thresholds and executive notification requirements based on incident severity, customer impact, duration, business criticality, security implications, and potential reputational or operational risk. Current escalation and major incident communication practices will be reviewed and formalized to ensure leadership receives timely, consistent, and actionable information during significant incidents.

16.c – EIS recognizes the need for a clearly accountable enterprise owner responsible for the effectiveness and continued maturity of incident management across CSS, DCS, and agency-facing services. The accountable owner will provide governance and oversight while operational teams remain responsible for executing incident management activities within their respective service areas.

16.d – EIS will require documented root cause analysis for significant incidents based on defined severity, impact, recurrence, risk, or executive escalation criteria. Corrective actions resulting from incident reviews will be centrally documented, assigned to accountable owners, given target completion dates, and tracked through closure. This work will also be aligned with the enterprise Problem Management framework to ensure recurring or systemic issues are appropriately transitioned from incident response into formal problem management.

16.e – EIS will establish enterprise-level incident management metrics and reporting to improve transparency, identify operational trends, measure service performance, and support continuous improvement. Metrics will be developed based on available and reliable data and may include mean time to detect, acknowledge, contain, restore, and resolve; incident volume and severity; recurrence rates; escalation rates; corrective action aging; and other measures determined appropriate through governance.

16.f – EIS will establish periodic testing and validation of incident communication methods, escalation pathways, contact information, leadership notification processes, and major incident coordination procedures. Testing may be incorporated into tabletop exercises, disaster recovery exercises, operational readiness activities, major incident simulations, or other scheduled exercises.

Please contact Shirlene Gonzalez at 971-803-1766, or Kip Memmott at 971-600-6090, with any questions.

Sincerely,



Terrence Woods
State Chief Information Officer
Director Enterprise Information Services



Secretary of State **Tobias Read**
Audits Director **Steve Bergmann**

Oregon Audits Division

255 Capitol St NE, Suite 180
Salem OR 97310
(503) 986-2255

audits.sos@sos.oregon.gov
sos.oregon.gov/audits