Secretary of State

Oregon Audits Division

Department of Administrative Services and Enterprise Information Services

EIS Has Established an IT Governance Framework but Must Do More Regarding Cybersecurity Management

September 2021

Report 2021-25

Secretary of State Shemia Fagan
Audits Division Director Kip Memmott

Secretary of State
Oregon Audits Division

Executive Summary

Department of Administrative Services, Enterprise Information Services

EIS Has Established an IT Governance Framework but Must Do More Regarding Cybersecurity Management

Why This Audit is Important

» Oregon cannot deliver public services effectively without effective information technology (IT) governance and cybersecurity controls.

» IT governance and security management and oversight in the state of Oregon requires coordination and cooperation between many entities, including the Governor, Enterprise Information Services (EIS), executive branch agencies, and other stakeholders.

» The statewide project portfolio in January 2021 included combined budgets of $1.4 billion.

» Cybersecurity remains a high-risk area for government entities as evidenced by increasing cyber-attacks affecting the public sector.

What We Found

1. **IT Governance**: EIS has developed a formal governance framework for new IT investments, and enterprise-level governance committees generally approve statewide IT documents that provide direction to agencies. However, cybersecurity risk governance should be established to define enterprise-level risk appetite and EIS should update documentation associated with subordinate governance entities. (p. 8)

2. **Cybersecurity Management**: EIS has established expectations for agency-level security management but lacks complete definition of centralized enterprise security services and roles it provides. It should enhance cybersecurity risk and vulnerability management programs. EIS should also enhance cybersecurity strategic planning and update key security management documents. EIS also lacks complete procedures to evaluate agency compliance with rules, policies, and standards each biennium, as required by statute. (p. 14)

3. **Communications**: EIS employs multiple communication channels but would benefit from definition of communication strategies. (p. 22)

What We Recommend

Our audit includes 10 recommendations to EIS. These are associated with improving documentation of governance, security management, and communications, as well as expanding enterprise risk and vulnerability management.

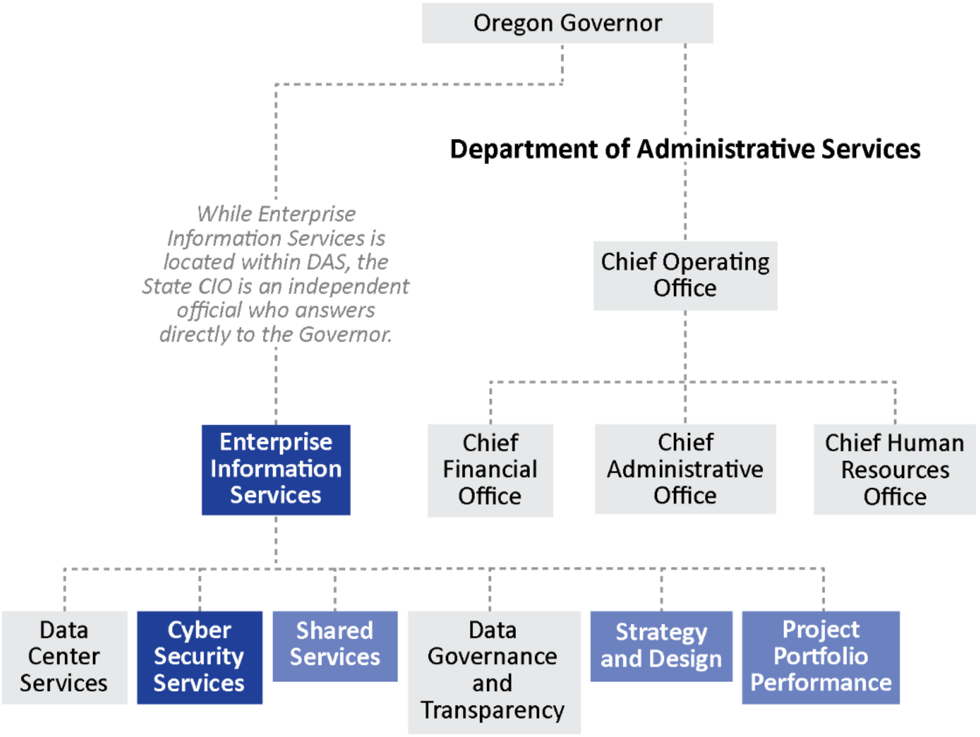
EIS agreed with six recommendations, partially agreed with three, and disagreed with one. The response can be found at the end of the report.

The Oregon Secretary of State Audits Division is an independent, nonpartisan organization that conducts audits based on objective, reliable information to help state government operate more efficiently and effectively. The summary above should be considered in connection with a careful review of the full report.

Introduction

The Department of Administrative Services (DAS) is the state's central administrative agency. DAS supports state agencies in the executive department by providing management frameworks and infrastructure for information systems and services, procurement, and other functions. The office of Enterprise Information Services (EIS), an organizational component of DAS, provides statewide information technology (IT) leadership for executive branch state agencies as well as maintaining statewide IT policy and oversight functions.

The State Chief Information Officer (CIO) reports directly to the Governor, similar to an agency head. EIS is funded primarily through assessments of state agencies based on the number of full-time equivalent positions, with a legislatively adopted budget for the 2021-23 biennium of nearly $122 million. Data Center Services, a section within EIS, has a separate budget of nearly $169 million for the 2021-23 biennium.


Oregon Governor
Department of Administrative Services
While Enterprise Information Services is located within DAS, the State CIO is an independent official who answers directly to the Governor.
Chief Operating Office
Enterprise Information Services
Chief Financial Office
Chief Administrative Office
Chief Human Resources Office
Data Center Services
Cyber Security Services
Shared Services
Data Governance and Transparency
Strategy and Design
Project Portfolio Performance

The six EIS sections provide unique services and have varied roles and responsibilities based on their functions within EIS as a whole, but they all operate under a unified mission, vision, and values to deliver a wide-ranging list of services.

- **Cyber Security Services (CSS):** CSS is the centralized security arm of EIS. This section encompasses governance, policy, procedure, and operations.
- **Project Portfolio Performance:** This section oversees major IT investments. It helps facilitate efficient decision-making, monitors adherence to policy and statute, and provides training and tools to assist agencies with IT investment initiatives.
- **Shared Services:** This section oversees several programs including E-Government, Quality Assurance, and Statewide Interoperability. It works to increase alignment between these and other existing enterprise programs. It houses the Project Management Office, which

manages internal EIS projects. It also manages long-term vendor relationships via the Basecamp program.[1]

- **Strategy & Design:** This section contributes to enterprise strategic technology initiatives and technology standards, processes, and policy development. Key initiatives include network and security modernization, enterprise cloud strategy, and the implementation of Microsoft 365, a suite of Microsoft Office and collaboration applications being rolled out to multiple agencies.
- **Data Governance and Transparency:** This section is charged with establishing Open Data standards and developing an enterprise data and information strategy.
- **Data Center Services:** The data center provides centralized computer services such as networking, email, backup, and server services.

The purpose of this audit was to assess whether EIS has established a governance framework to cover its statutory responsibilities, to review statewide IT security management and oversight, and to evaluate whether communication of expectations, requirements, services, and roles and responsibilities was defined, developed, and implemented. Our primary focus was on the activities of CSS, but our objectives covering governance and communication also considered the activities of Shared Services, Strategy and Design, and Project Portfolio Performance.

Governance consists of multiple layers and has multiple definitions

Oregon law stipulates "[t]he State Chief Information Officer shall implement and maintain an information technology governance program for the executive department."[2] The statute does not define "governance."

The concept of governance incorporates many possible components and definitions across several different layers of responsibility, from the Governor to agency program managers. Part of our audit work included examining some of these definitions and layers and applying them to the environment under which executive branch agencies in the state of Oregon operate. We also reviewed statutes and identified governance-related responsibilities assigned to the State CIO for the oversight, integration, acquisition, development, planning, security, and use of information resources in the executive department.

Enterprise governance sets strategic direction across the enterprise

For this audit, the first layer of governance we considered is enterprise governance. The overarching goal of enterprise governance is to provide strategic direction, along with ensuring objectives are achieved, ascertaining risks are managed appropriately, and verifying enterprise resources are used responsibly.

"Enterprise" is a general term that, for the state of Oregon, could be defined to encompass the entire state, including private industry as well as state and local government. Indeed, certain portions of statute refer to these other entities when discussing the context of security in Oregon. However, for practical purposes relating to our audit objectives, we defined "enterprise" as executive branch agencies over which the Governor, and subsequently the State CIO, has authority.

This audit defines "enterprise" as the executive branch agencies over which the Governor, and subsequently the State CIO, has authority.

[1] Basecamp is a single IT information portal leveraging statewide agreements to provide access to IT solutions across the state. See prior audit report 2018-45.

[2] ORS 276A.203(4)(a)(B)

Enterprise IT governance aims to ensure IT supports and enables the enterprise strategy and achievement of enterprise objectives and includes IT portfolio, cybersecurity, and cybersecurity risk governance

Beneath enterprise governance is enterprise IT governance. The goals of IT governance are to ensure IT sustains and extends enterprise strategies, goals, and objectives, and ensure IT capabilities are provided efficiently and effectively. Within the state of Oregon, the Governor and State CIO work together to provide strategic direction for IT within the enterprise. Any IT activities or plans throughout the enterprise should be in support of such direction, which means that enterprise IT governance also has an oversight role.

Enterprise IT governance is further supported by related, specifically focused governance areas. When evaluating what enterprise IT governance in Oregon should include, in alignment with the overall definitions of enterprise IT governance and the specific responsibilities assigned to the State CIO, we considered three areas: portfolio, cybersecurity, and cybersecurity risk governance.

The first focus area identified is IT portfolio governance. As a major component of enterprise IT governance, it focuses on evaluating proposed IT investments for alignment with strategic objectives. It also helps determine where to apply the enterprise's limited resources. Oregon has specific statutes defining how IT portfolios should be managed to help reduce the risks associated with IT related projects.[3]

The second focus area is cybersecurity governance. Again, definitions vary, but common themes are that this area of governance should:

- Ensure information cybersecurity strategies support business objectives and help reduce risks;
- Formulate rules and procedures to help define expected best practices to follow; and
- Assign responsibility for cybersecurity roles.

Cybersecurity risk governance is our third focus area. It should help establish risk management priorities and guide the risk management strategy to ensure alignment with these priorities. This can include defining the enterprise-level cybersecurity risk appetite to guide risk mitigation activities or definition of risk appetite at lower levels, such as state agencies.

Cybersecurity risk governance
Cybersecurity risk governance should help establish risk management priorities and guide the risk management strategy to ensure alignment with these priorities. This can include defining the enterprise-level cybersecurity "risk appetite" – the level of risk an organization is prepared to accept in pursuit of its objectives.

Oregon's IT governance model and central IT organization evolved over several decades

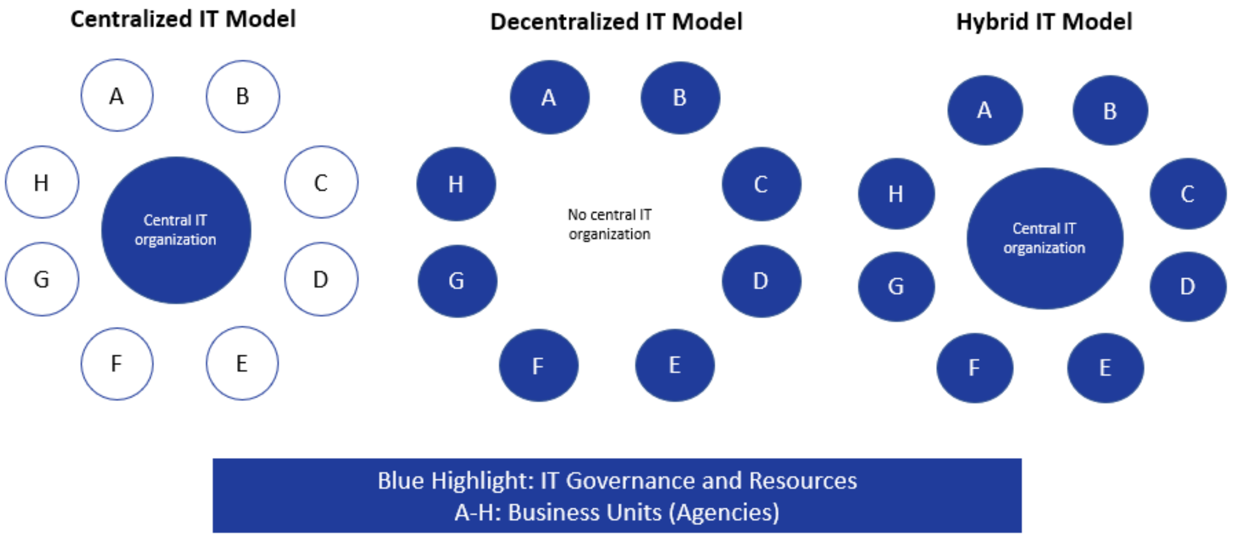
Within the context of overall governance, there are three major IT governance models in use in different states. These are centralized, decentralized, and hybrid governance and management of IT. Over the last few decades, Oregon's IT governance model has evolved from a mainly decentralized environment to a hybrid model, with some recent expansion of centralized responsibilities at EIS.

[3] ORS 276A.233

States and other organizations commonly employ centralized, decentralized, and hybrid IT organizational and governance models

The University at Albany's Center for Technology in Government explains three models for distributing authority in its report, "Enterprise IT Governance in State Government: State Profiles": centralized, hybrid, and decentralized. In a centralized governance structure, sole authority and decision-making power are assigned to a central IT organization, resulting in greater control over IT resources at the price of decreased flexibility. A decentralized governance structure gives all IT decision-making power to agency-level IT departments, which gives individual departments flexibility needed to react to their environment, but also results in a lack of coordination across the state. In a hybrid structure, the authority over IT decision-making is distributed between the central IT organization and the agency IT departments. This arrangement offers the flexibility needed for individual agencies, while also retaining some degree of centralized control over IT.[4] These structures may also apply to IT service provision in an enterprise environment.

Figure 1: Entities frequently adopt one of three typical models for IT governance and resources – centralized, decentralized, and hybrid



Organizations choose a model depending on their needs and various advantages or disadvantages associated with each one. For instance, in a decentralized model, more resources may be needed, since functions and services are not shared, and therefore would require these services to be provided at each entity. A centralized model may reduce the need for resources since functions are more readily shared. In a hybrid model, the challenge lies in balancing the central resources required with the decentralized needs. On this spectrum, Oregon operates under the hybrid governance model, though it has been trending from mainly decentralized towards increasingly centralized.

Centralized IT responsibilities have evolved in Oregon

Oregon has operated under a partial hybrid model with regard to information systems for many decades. In 1967, Oregon Laws charged a central Department of Finance with devising plans for the "acquisition, installation, and use of electronic or automatic data processing equipment by the state

[4] Hrdinová, Jana, Natalie Helbig, and Anna Raup-Kounovsky. 2009. *Enterprise IT Governance in State Government: State Profiles*. Albany: University at Albany Center for Technology in Government.

government and all agencies thereof." It also required this department to consult with state agencies when devising those plans. Additional laws in the 1980s and 1990s expanded this authority. In 1991, a "legislative finding" was added that mentioned the need to establish central management structures for the security of information resources, though this did not assign responsibility for creating these structures to any agency. After its creation in 1993, DAS was assigned the responsibility to adopt policies, standards, and guidelines to plan for, acquire, implement, and manage the state's IT resources.

Since then, major changes that greatly expanded the staffing and responsibilities of DAS over state IT have pushed Oregon closer to centralized governance and services, while still retaining the overall hybrid model. The first of these was the consolidation of 11 data centers operating at different agencies into a state data center in a project that began in 2004 and finished in 2007. At the time the data center began operations, it operated as its own unit under DAS rather than being placed with other central IT policy and planning functions in existence at that time.

Additionally, in 2005, the Oregon Legislature passed House Bill 3145, which assigned significant responsibility for statewide information security to DAS. Per the bill: "(DAS) has responsibility for and authority over information systems security in the executive department, including taking all measures reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. (DAS) shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures."[5] The Enterprise Security Office (ESO) was created by the beginning of the 2007-09 biennium and was responsible for developing statewide information security policies and practices.

Further major changes took place starting in 2013. First, House Bill 3258 established the office of the State CIO within DAS and assigned IT-related responsibilities to the State CIO instead of DAS. In 2014, the State CIO, in cooperation with the Legislative Fiscal Office, established the stage gate process — an incremental funding and project oversight model for major IT initiatives exceeding $1 million or posing substantial risk.

In March 2015, the Governor reorganized leadership over statewide IT policy and operations, first assigning temporary operational responsibility for the data center to the State CIO; House Bill 3099 made this responsibility permanent. This bill also designated the State CIO as an independent official, directly responsible to the Governor as the primary advisor on statewide IT policy and operations. This change brought both the data center and ESO under the umbrella of what is now named EIS.

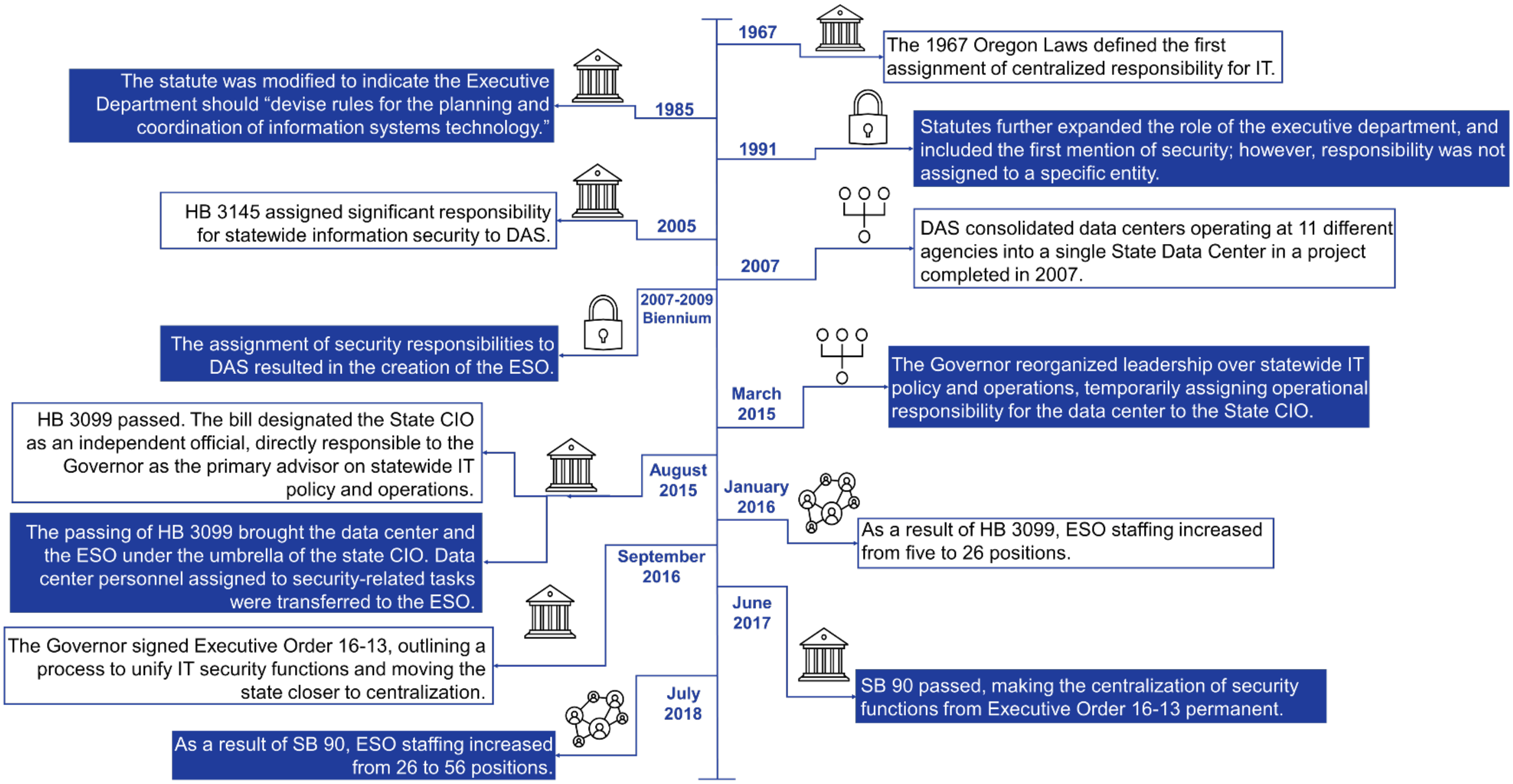
In September 2016, the Governor signed Executive Order 16-13, which outlined a process to unify cybersecurity functions for the majority of state agencies. [6] The order directed executive branch agencies, as defined in statute, to consolidate security functions and staffing into EIS and to work with the newly consolidated group to develop and implement security plans, rules, policies, and standards adopted by the State CIO. This order was made permanent by the passage of Senate Bill 90 in June 2017. [7] The bill transferred 30 positions from state agencies and created five additional positions within ESO. The various expansions of security responsibility and consolidation of personnel resulted in the staffing of ESO increasing from five mainly policy-related positions in 2015 to 56 positions as of July 2018.

Despite these changes, the fundamental nature of the hybrid governance model remained in Oregon. Documents from 2018 indicate that full centralization of IT in the state was considered and

[5] House Bill 3145
[6] Executive Order 16-13: Unifying Cyber Security in Oregon
[7] Senate Bill 90

rejected. Agencies still retain primary responsibility for their internal IT governance and management and EIS maintains enterprise-wide governance, oversight and planning responsibilities while also providing central services through its various sections. The statutory unification of security functions and staff have placed more operational responsibilities for security at EIS, though in practice many responsibilities still lie with the agencies.

Figure 2: The timeline of key events for IT governance and operations in Oregon spans from 1967 to 2018



1967 — The 1967 Oregon Laws defined the first assignment of centralized responsibility for IT.

1985 — The statute was modified to indicate the Executive Department should "devise rules for the planning and coordination of information systems technology."

1991 — Statutes further expanded the role of the executive department, and included the first mention of security; however, responsibility was not assigned to a specific entity.

2005 — HB 3145 assigned significant responsibility for statewide information security to DAS.

2007 — DAS consolidated data centers operating at 11 different agencies into a single State Data Center in a project completed in 2007.

2007-2009 Biennium — The assignment of security responsibilities to DAS resulted in the creation of the ESO.

March 2015 — The Governor reorganized leadership over statewide IT policy and operations, temporarily assigning operational responsibility for the data center to the State CIO.

August 2015 — HB 3099 passed. The bill designated the State CIO as an independent official, directly responsible to the Governor as the primary advisor on statewide IT policy and operations.

The passing of HB 3099 brought the data center and the ESO under the umbrella of the state CIO. Data center personnel assigned to security-related tasks were transferred to the ESO.

January 2016 — As a result of HB 3099, ESO staffing increased from five to 26 positions.

September 2016 — The Governor signed Executive Order 16-13, outlining a process to unify IT security functions and moving the state closer to centralization.

June 2017 — SB 90 passed, making the centralization of security functions from Executive Order 16-13 permanent.

July 2018 — As a result of SB 90, ESO staffing increased from 26 to 56 positions.

Leadership changes resulted in reorganization of EIS and Senate Bill 90 expanded some security services

EIS has also experienced several significant leadership changes in the last several years. Both the State CIO and the State Chief Information Security Officer (CISO) left their positions in 2018 and new leadership arrived. The new State CIO formally took over in December 2018 and, in the following year, reorganized and rebranded EIS to reflect its role as a service organization. With the reorganization of EIS in 2019, its divisions were renamed. The ESO was renamed CSS. The current State CISO began in the position in July 2019.

CSS has three major sections. The Network Security section performs technical operations, such as managing firewalls and providing VPN services.[8] This group formerly operated at the state data center; the functions and personnel moved under CSS as a result of House Bill 3099 in 2015. The manager of this group reported they had no specific enhancement based on the movement of personnel from Senate Bill 90 or Executive Order 16-13.

The second section, named the Security Operations Center (SOC), had also already been established prior to Senate Bill 90 or Executive Order 16-13. The section has a group focused on vulnerability management, which supports the scanning tools and assists agencies with their use as well as

[8] VPN, which stands for virtual private network, is a method of establishing a secure connection to the internet.

providing some enterprise-level reporting. Additionally, the SOC provides monitoring and detecting services, including maintaining the implementation of an intrusion detection system and monitoring logs through a Security Information and Event Management tool. A threat intelligence function monitors security threats through use of external services such as the Multi-State Information Sharing and Analysis Center.

The SOC also recently implemented a new network filtering service to further protect agencies against known threats. It also provides enterprise-level security incident response services. Per discussion, these functions have been enhanced through the infusion of agency personnel, but most of the basic functions had existed prior to the Executive Order and Senate Bill 90.

The third section of CSS, called Governance, Risk, and Compliance, houses the new major functions that did not previously exist within CSS. This section is also currently focused on providing services to agencies. Its Risk section conducts risk and cybersecurity assessments of agencies based on the controls defined in CIS 7.1[9] and other negotiated criteria. The Business Enabling group is intended to be a resource for agencies by providing Business Information Security Officers (BISO), who are generally available upon request for security-related activities such as helping to develop agency-specific security policies or mitigating security risks. This group also has a major role in working with agencies implementing new IT investments by consulting on security requirements for new systems. Finally, the Security Awareness function includes an individual who coordinates and tracks statewide information security awareness training.

Some changes were driven by past project failures and increased threats to information security

Several of the more recent changes to Oregon laws and reorganization of enterprise IT governance, security, and oversight were in part driven by the need to address identified weaknesses in processes. For example, the expansion of oversight for projects and new investments through the introduction of the stage gate process was in large part a direct response to failed investments, such as Cover Oregon in 2013. In addition, the decision to place the state data center under the direct authority of the State CIO in 2015 came after several Secretary of State audits critical of security at the state data center, and a publicized security breach. The 2016 centralization of cybersecurity – codified in SB 90 – came from a deeper understanding of the ever-changing threat landscape.

Data Center Security Warnings Issued:

2006 Public Audit
2008 Public Audit
2008 Confidential Audit
2008 Consultant Report
2009 Public Audit
2009 Confidential Audit
2010 Public Audit
2010 Public Security Audit
2010 Confidential Audit
2012 Public Audit
2012 Confidential Audit
2015 Public Audit

As the laws and governance evolved, so did the name and organization of the central IT organization in Oregon, now referred to as EIS. The changes also included modifying names and structures within individual units, such as changing the name of the unit primarily tasked with cybersecurity. In general, these changes were not unreasonable. As noted, many of them were done in response to identified issues or increased understanding of threats. Other change catalysts included the differing ideas and priorities of state leaders over the last decade, including those filling the role of the State CIO. The changes and their effects on agencies and their perceptions demonstrate the need for clear and transparent definition and structure of IT governance for the state so that stakeholders understand how decisions are made.

[9] Center for Internet Security

Audit Results

We found that enterprise governance consisting of the Governor and State CIO work together to develop strategic direction for state IT, in consultation with state agency leaders. EIS has also developed an IT governance program that addresses the oversight, integration, acquisition, development, planning, and security of executive branch agency information resources for new IT investments. In addition, EIS develops or leads workgroups as needed to develop statewide IT policies, standards, or other documents for approval by the enterprise governance groups. However, some supporting governance group definitions are outdated and should be clarified. In addition, enterprise-level cybersecurity risk governance should be established to provide guidance to enterprise and agency-level risk management and define the state's risk appetite – the level of risk the state is willing to accept.

We also found EIS has fulfilled many of its responsibilities associated with security management. It has established standards, developed a security plan for agencies to adopt, and published policies. However, we also concluded it has not yet fully documented enterprise-level security services to demonstrate how services provided at the enterprise level help to secure the enterprise environment, nor has it fully clarified roles and responsibilities for security activities. It has not yet fully implemented centralized risk and vulnerability management to help ensure that critical risks encountered by agencies are being timely remediated. Some key security documents are also outdated, and EIS does not have robust mechanisms in place to ensure agencies are complying with rules, policies, and standards.

We also found EIS has developed multiple communication channels to inform agencies of needed information regarding EIS expectations, requirements, services, and roles and responsibilities. However, these communication efforts are largely ad hoc and would be enhanced by more formal procedures to define communication strategies for its various stakeholders.

IT governance is in place for the enterprise and for new investments, but additional work is needed to implement cybersecurity risk governance

Overall strategic plans at the Governor's Office and EIS levels have provided guidance for IT activities to occur at EIS and to help guide additional strategic planning at the agency level.

Organizational structures in the form of the Enterprise Leadership Team (ELT) and a supporting committee have been established to provide high-level governance for Oregon executive branch agencies. These groups perform functions such as reviewing and approving statewide policies and standards, as well as prioritizing projects proposed by agencies for input to the budgetary process.

At the EIS level, there are many policies and procedures to support a robust IT governance process for new IT investments. While some of these are new efforts, the overall process has been in place since 2014 and has undergone improvements over time. We have audited the details of the process in prior audits and current work did not focus on the areas already reviewed.[10]

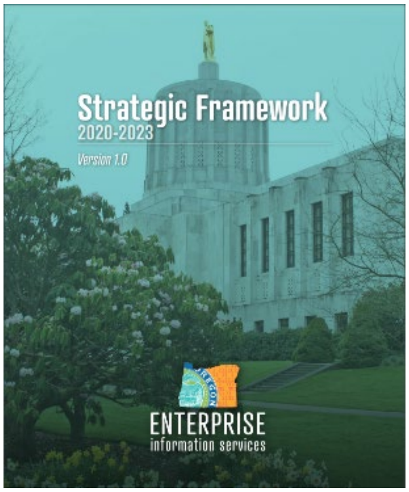
Additional governance committees or boards to support the higher-level governance groups are less well-defined or outdated and would benefit from clarification. Furthermore, enterprise-level cybersecurity risk governance has not yet been established.

[10] See audit reports 2015-06, 2018-45, and 2020-18.

Enterprise governance provides strategic direction

For Oregon executive branch agencies, enterprise-level governance is led by the Governor, supported by the State Chief Operating Officer, who heads DAS, and the State CIO, who leads EIS. In addition, these two roles co-chair the ELT, a group of over 20 state agency leaders, which provides shared leadership for the management of state government. We considered overall enterprise governance only as it related to how it provided overall strategic direction for enterprise IT.

In 2018, the Governor's Office issued multiple "Action Plans for Oregon" with various focus areas. For IT, the plan was co-authored by the Governor, the Chief of Staff, and the State CIO. The plan is titled: "User-friendly, Reliable and Secure: Modernizing State Information Technology Systems and Oversight."[11]



To support the strategies in the Governor's Action Plan, EIS published the "Enterprise Information Services Strategic Framework" after consulting with Oregon state agency business leaders, state IT leaders from other states, private sector IT leaders, and the Governor's Office.[12] This document provides an overview of EIS and its programs, as well as communicating the overall mission, vision, and high-level objectives and goals for EIS.

Overall, the objectives and goals of this document support the strategies discussed in the Governor's Action Plan. Some of these objectives and goals require actions that need to be taken by individual agencies with assistance from EIS, such as developing IT strategic plans that align to business strategic plans. Others are more focused on efforts at EIS to develop statewide strategies for individual areas, such as cloud or data.

These two documents provide high-level direction for defining additional actions to be taken by EIS for the enterprise and to assist in agency planning. In addition, the development of the Strategic Framework reflects the commitment of EIS leadership to soliciting feedback from agencies for enterprise IT strategic planning.

Appropriate enterprise-level IT governance structures are in place to review and approve statewide IT policies and standards, but EIS should clarify the purpose and status of subordinate governance groups

Major components of governance consist of organizational structures as well as policies, plans, and standards to provide direction and requirements for those being governed.

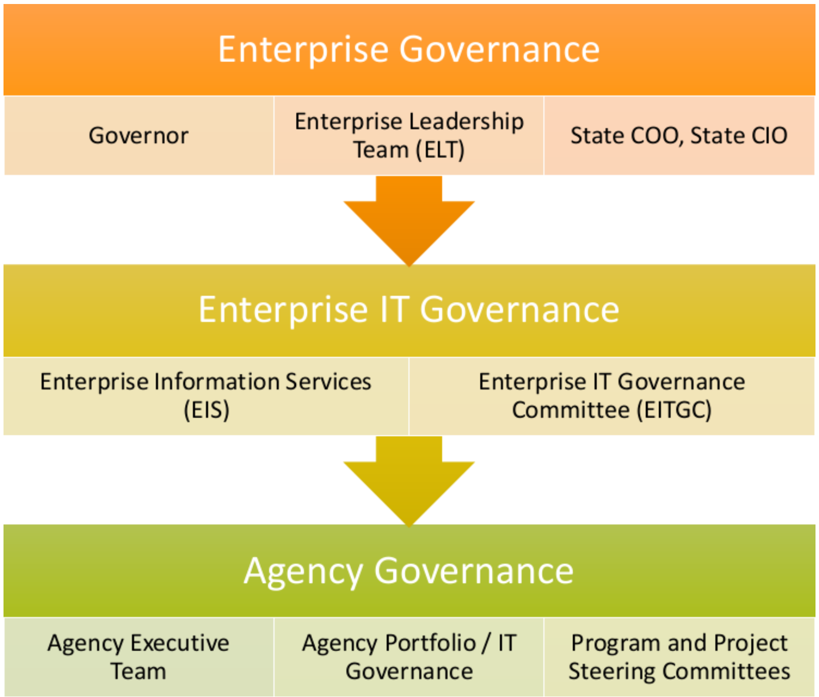
In Oregon, the State CIO uses the ELT to help guide enterprise IT governance. While the ELT structurally operates at the enterprise level, EIS managers stated it reviews and approves statewide IT policies and standards. This approach is intended to encourage agency agreement with the enterprise-level decisions or direction.

A second organizational structure is the Enterprise IT Governance Committee (EITGC), which is a subset of the ELT. It consists of six to 10 directors from agencies, boards, or commissions of different sizes, and also includes the State CIO and Deputy State CIO. The mission of this committee is "to provide strategic guidance and recommendations to the ELT to inform and support the State's

[11] User-friendly, Reliable and Secure: Modernizing State Information Technology Systems and Oversight
[12] EIS Strategic Framework

Enterprise IT Vision." As such, the EITGC reviews and approves relevant statewide IT documents prior to their submission to the ELT.

Figure 3: EIS defines three Oregon governance tiers and identified committees


Enterprise Governance
Governor
Enterprise Leadership Team (ELT)
State COO, State CIO
Enterprise IT Governance
Enterprise Information Services (EIS)
Enterprise IT Governance Committee (EITGC)
Agency Governance
Agency Executive Team
Agency Portfolio / IT Governance
Program and Project Steering Committees

Source: EIS presentation to the Joint Legislative Committee on Information Management and Technology on February 10, 2021.

The EIS website, the EITGC charter, and the Statewide Information Security Plan refer to the existence of supporting or subordinate governance or advisory groups that are intended to provide input to these higher-level governance groups or to EIS. However, some of these subordinate groups have been renamed and others have been eliminated, as they were judged as no longer necessary. The associated documentation has not been updated to clarify the current status and purpose of these subordinate groups, which detracts from the transparency of how enterprise IT governance is conducted in Oregon.

Overall, we concluded the high-level governance structures provide a reasonable approach to providing enterprise IT governance. They ensure agency directors, as the business leaders of their organizations, have input into enterprise-level requirements to which their agency would be subject, as is needed for a hybrid governance model. However, clarifying the status and role of subordinate governance or advisory groups would improve transparency.

EIS IT governance roles and procedures support new IT investments

A more focused area of overall enterprise IT governance is enterprise IT portfolio governance. This area focuses on ensuring that new IT investments support overall business objectives, that the investments warrant the application of limited resources, and that the projects to implement the investments are managed appropriately. State statutes further support the importance of overseeing new IT investments by assigning the State CIO specific responsibilities associated with IT portfolio-based management and inventory, along with requiring quality assurance reviews of IT initiatives undertaken by executive branch agencies.[13]

[13] ORS 276A.233 and ORS 276A.223(2)(a)

The EIS Strategic Framework specifically defines IT governance as it relates to new IT investments. The document notes that "IT governance is about accountability and is a formalized process for making, communicating, and implementing IT investment decisions." It is around this definition that EIS has directed resources most associated with governance activities. Specifically, the Project Portfolio Performance section in EIS provides oversight and portfolio management for IT investments for executive branch agencies under the authority of EIS.

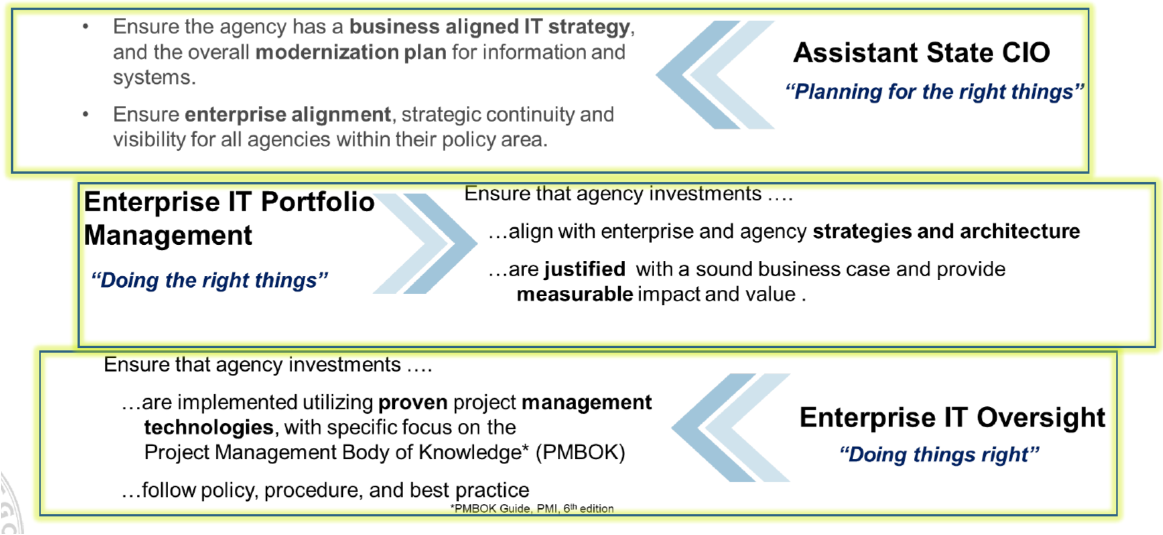
Given past major IT project failures and large dollar figures associated with funding major new IT investments, this is an important focus area. The Audits Division has conducted several audits associated with the "stage gate" process, a joint process originally developed by EIS and the Legislative Fiscal Office in 2014 to approve and oversee certain IT projects. For this audit, we relied on our past audit results of these governance processes along with a review of some new updates not covered in previous audit results. Overall, these procedures are among the most mature at EIS and this area of governance appears strong, though not without challenges.

Agencies are responsible for determining whether they need a new IT investment. Ideally, agency-level governance procedures should analyze agency-specific business needs and propose new IT investments to support those needs.

Two groups within EIS may assist with this process. First, during the 2019-21 biennium, the Legislature approved six new positions for Assistant State CIOs. These positions may assist agencies with both IT strategic and modernization planning. As indicated in EIS documents, Assistant State CIOs are involved in helping agencies to "plan for the right thing."

Second, Senior IT Portfolio Managers from the Project Performance Portfolio section also can assist agencies with planning. These individuals are involved in the stage gate process as the initial evaluator of agency IT investment ideas and can assist agencies in developing strong business cases. EIS documents indicate Enterprise IT Portfolio Management, which is led by the Senior IT Portfolio Managers, is involved in helping agencies "do the right thing."

Figure 4: EIS has multiple roles in enterprise IT investment governance



- Ensure the agency has a **business aligned IT strategy**, and the overall **modernization plan** for information and systems.
- Ensure **enterprise alignment**, strategic continuity and visibility for all agencies within their policy area.

Assistant State CIO

"Planning for the right things"

Enterprise IT Portfolio Management

"Doing the right things"

Ensure that agency investments ….

…align with enterprise and agency **strategies and architecture**

…are **justified** with a sound business case and provide **measurable** impact and value .

Ensure that agency investments ….

…are implemented utilizing **proven** project **management technologies**, with specific focus on the Project Management Body of Knowledge* (PMBOK)

…follow policy, procedure, and best practice

*PMBOK Guide, PMI, 6th edition

Enterprise IT Oversight

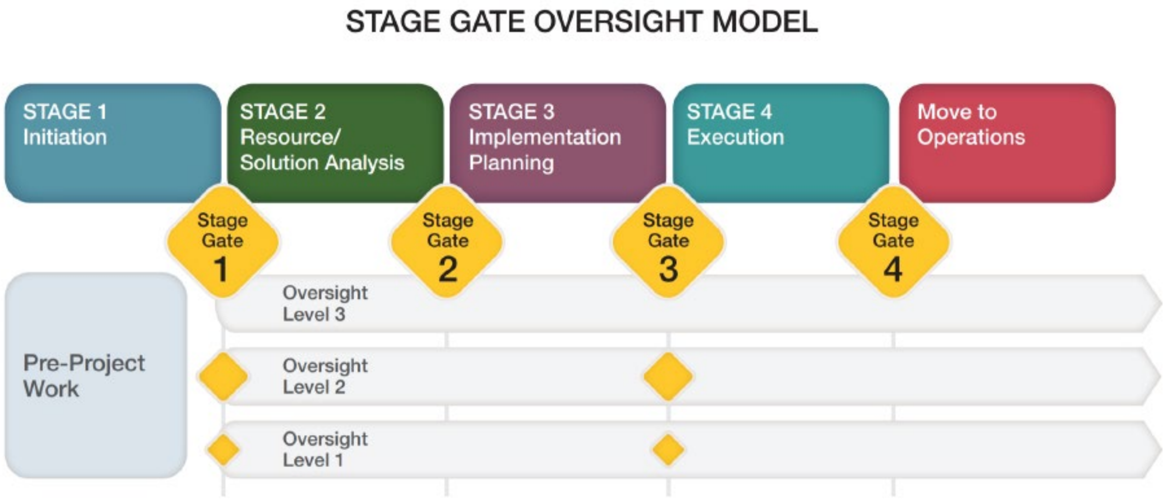
"Doing things right"

Source: Presentation to Public Safety Policy Area representatives from an Assistant State CIO.

Further elements in the IT investment governance process managed by EIS occur at more detailed levels. Throughout the project, based on stage gate requirements, agencies submit further foundational project documents to EIS for review and approval by Oversight Analysts, also housed in the Project Portfolio Performance section. These Oversight Analysts are charged with determining which detailed oversight level is warranted, determining which artifacts to request, reviewing artifacts, and recommending stage gate endorsement to the State CIO. Ultimately, this oversight group is intended to fulfill a third governance concept to "do things right."

In response to prior audits and agency feedback, in June 2020, EIS updated its stage gate policies and procedures to allow for different levels of oversight based on different types of investments and associated risk levels. Under this model, less complex projects would be subjected to fewer oversight requirements than more complex projects. Depending on the level of oversight, agencies would then be required to develop different types of foundational project documentation. The agencies then submit these documents to EIS for review and approval at different key points during the project, known as gates.

Figure 5: EIS has updated the stage gate oversight model for projects with different oversight levels



Source: Presentation by EIS on May 21, 2020, to inform agencies of the new oversight process.

For major IT projects that require individual budget requests during the legislative process, higher level governance groups are also involved in reviewing and prioritizing the proposed projects. This practice was first adopted during the 2019-21 biennium and was adjusted for the 2021-23 biennium. Specifically, agencies will score their proposed projects using an established set of criteria available on the EIS website. These scores and associated project business cases will be presented to the EITGC for review. The committee, with feedback from Senior IT Portfolio Managers, will evaluate and potentially adjust the priority scores and send this list to the DAS Budget Office for further evaluation. Ultimately, agencies include requests to fund major IT projects in their budgets, and the Legislature determines whether to fund these efforts.

These procedures are designed to ensure major IT investments are based on sound business cases; support the Governor's Action Plan, EIS Strategic Framework, or agency strategic plans as necessary; and align with other IT investments. The goals of these procedures are to ensure IT investments will provide value for the enterprise and IT resources associated with the projects are appropriately assigned.

Prior audits have identified some challenges with the oversight process, including consistency in applying evaluation criteria for project deliverables. However, overall, these processes represent formal, defined methodologies for evaluating and overseeing IT investments, both at the EIS governance level and the EITGC.

Cybersecurity governance occurs within the IT governance structure, but enterprise cybersecurity risk governance is not yet established

Two other focus areas of enterprise IT governance relate to cybersecurity governance and governance of cybersecurity risk. Cybersecurity governance is focused on ensuring security initiatives support business objectives to reduce risks, formulating rules and procedures, and assigning responsibility for security roles. Cybersecurity risk governance should exist to provide an enterprise-wide view of risk appetite to provide guidance to enterprise and agency-level risk management.

Although a leading practice, EIS has not developed a separate governance entity to specifically consider security-related governance elements but uses other means to manage the major functions of cybersecurity governance. EIS managers indicated the existing governance structures of the ELT and EITGC review and approve statewide policies and standards. These documents are developed by EIS or by temporary, task-oriented workgroups. EIS also has an internal governance board that considers proposed initiatives, including those for enterprise information security, and any project proposals are subject to the same stage gate processes discussed in the previous section. As such, many of the major elements associated with cybersecurity governance are being addressed by existing structures.

However, cybersecurity risk governance, which is a subset of cybersecurity governance, is not yet being sufficiently addressed. EIS began work on establishing an enterprise-level cybersecurity risk governance structure in early 2019. It drafted a charter for a potential governance group, a statewide risk management program plan, and policy for risk management. However, these documents have not yet been adopted or approved and the activities outlined have not been implemented. For example, there is no enterprise-level risk monitoring strategy, and there have been no priorities established for responding to risks. No existing group currently fulfills the functions described in these documents.

Enterprise Cybersecurity Risk Governance Not Implemented
EIS has not established an enterprise-level cybersecurity risk governance group. It has drafted documents to establish a group, but no existing group currently fulfills the functions described in these documents.

EIS managers indicated a major reason for delays in further development or approval of these plans is their desire to first procure and implement a statewide application that can be used by EIS and agencies to track identified risks and mitigation activities. Activities on a project to procure an Enterprise Integrated Risk Management tool began in 2018, but the project has experienced some delays and the tool was only procured on June 24, 2021. Further work will be needed to configure and implement the tool at CSS and at agencies.

While implementing a tool will be beneficial for collecting data which can be used to manage and report on security risks, the most critical governance need is to define and document an enterprise-level risk appetite and strategy. Definition of risk appetite should guide additional prioritization of activities to mitigate risks, either at the agency level or the enterprise level.

EIS should develop and update security management documentation and enhance enterprise security management oversight activities

Security management is focused on defining and implementing best practices at several levels of an organization. CSS has appropriately defined security expectations for agencies through its publication of key documents. However, it should do more to document how services it provides help ensure enterprise-wide security, manage enterprise security risks, formally document its IT security strategic plans, and update several outdated security management documents.

Major security management documents provide guidance to agencies

Organizations should establish a security management program that covers certain key elements. These include periodic risk assessments, adequate policies and procedures, subordinate information security plans, security awareness training, management testing and evaluation, vulnerability and risk mitigation procedures, and security incident procedures.

Security management should also be addressed at different levels within an organization. For the IT structure under which Oregon executive branch agencies operate, these consist of the enterprise level, as led by EIS; the agency level, as determined by individual agencies; and the system level, which would consist of individual systems operating at an agency. The responsibilities at the EIS level are confirmed through key statutes.[14]

Statewide Information and Cybersecurity Program documents

Components of the security program are detailed in the following documents:

- Statewide Information Security Plan
- Statewide Information and Cyber Security Standards
- Statewide Information and Cyber Security Policies
- Agency Information and Cyber Security Plans and Policies
- System Security Plans

Source: 2019 Statewide Information and Cyber Security Standards

For enterprise security management, EIS, in coordination with agencies, has developed several key documents to define security expectations and requirements at the enterprise level, though these expectations apply to the agency and system levels. These consist of the Statewide Information Security Plan, published in August 2018; the Statewide Information and Cyber Security Standards, published in June 2019; and a variety of statewide information and cybersecurity policies.[15]

The security plan outlines a set of security expectations directed specifically at agencies for areas they control. Agencies are expected to either adopt the plan as their own, with any deviations or amendments documented, or develop their own plan that meets or exceeds the requirements listed. The security standards further support the security plan and define different levels of controls required for applications containing data with different data classifications. In addition, there are 14 statewide IT or security-related policies, 11 of which are referenced in the security plan. The policies define additional requirements and expectations for agencies to follow.

Collectively, these documents provide guidance on the minimum expected controls for agencies to implement to protect their systems and data. They specify expectations that agencies will conduct risk assessments, develop agency-level policies and procedures as needed, and develop subordinate security plans. They also address requirements for agencies to ensure their personnel receive security awareness training. They include guidance for how agencies should ensure compliance with statewide information security policies, plans and standards and provide requirements for a number of other areas including asset management, information classification, human resources security, and incident response. As such, CSS is fulfilling its primary statutory responsibility to develop security plans, standards, policies, and procedures in many critical areas.

CSS is fulfilling its primary statutory responsibility to develop security plans, standards, policies, and procedures in many critical areas.

[14] ORS 276A.300(2): "The State Chief Information Officer has responsibility for and authority over information systems security in the executive department, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall, after consultation and collaborative development with agencies, establish a state systems information security plan and associated standards, policies and procedures."

[15] Statewide Information Security Plan, Statewide Information and Cyber Security Standards V1.0, and Statewide policy page

As indicated, security management should include definition of actions taken by all levels of an organization. There is no additional enterprise-level security management plan to describe the controls in place at the enterprise level. Instead, CSS indicated these controls are best expressed through definition of the services it provides to agencies. However, CSS should further define and document the services it provides to help ensure enterprise security and clarify security roles and responsibilities between state entities.

CSS services and associated roles and responsibilities have been generally defined but should be expanded

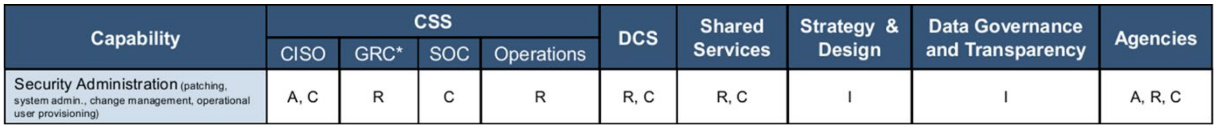
Organizations should establish IT-related roles and responsibilities for all personnel in the enterprise, in alignment with business needs and objectives, and clearly delineate responsibilities and accountabilities, especially for decision making and approvals. Service organizations should also define the services provided to its customers.

In late 2019, CSS engaged a vendor to develop a chart to define roles and responsibilities between different EIS sections and agencies, and a security service catalog, as required by a budget note in the 2019 legislative session. While review and approval of these documents was delayed through much of 2020 due to the COVID-19 pandemic, in March 2021, CSS published an initial version of its service catalog that provides some definition of the information security services it provides. In April 2021, CSS also published the first version of a quarterly metrics report to help describe the extent to which its services are being used by agencies and a few measures of whether these services are helping to manage risk. The vendor also developed a RACI chart[16] to identify roles and responsibilities. The chart includes different "capabilities," representing a task or service, then defines which high-level entity within EIS, including the three CSS subsections as well as the other divisions within EIS, or agencies are responsible, accountable, informed, or consulted.

While these efforts represent a good starting point, further work should be done to refine the descriptions and provide additional information. Some of the services described in the initial published catalog are not yet available, and the document does not indicate whether these services are expected to be provided at all, or when. The initial service catalog does not always provide information to agencies regarding whether these services are provided for all customers or whether they need to be requested. It also does not consistently contain instructions on how to request those services.

In addition, the RACI chart has been generally shared with agencies but has not yet been published. It also does not clearly delineate some of the responsibilities.

Figure 6: An example from the RACI chart showing multiple entities as Responsible and Accountable



Capability	CSS				DCS	Shared Services	Strategy & Design	Data Governance and Transparency	Agencies
	CISO	GRC*	SOC	Operations					
Security Administration (patching, system admin., change management, operational user provisioning)	A, C	R	C	R	R, C	R, C	I	I	A, R, C

Source: RACI chart deliverable.

Common guidance for RACI charts is that a single capability should not have two or more entities assigned as either "responsible" or "accountable." For the current RACI chart, 23 of the 69 capabilities include more than one "responsible" entity, and 16 included more than one "accountable" entity. The chart also does not further define which role within the high-level EIS section might have responsibility for each area. For example, Shared Services is assigned

[16] A RACI chart is a diagram that identifies key roles and responsibilities of different groups for different tasks by highlighting which role or group is Responsible, Accountable, Consulted, or Informed.

responsibility or accountability for nine areas, but neither the RACI chart nor any supporting documents identify in which of the six business areas within Shared Services these responsibilities lie.

Without a complete definition of available services, customers are less likely to know how enterprise-level services help to support their efforts to secure their own environment. It could also lead to a false sense of security if customers believe CSS is providing a service that it is actually not providing. Without clear and transparent definition of roles and responsibilities, required actions may not be taken because there is uncertainty over which entity is expected to fulfill that role. Additionally, if roles and responsibilities are unclear, the possibility exists of duplicating efforts and thus wasting resources on actions already performed.

Clear documentation of roles and responsibilities between CSS and the agencies has been a challenge since the transition of personnel from agencies to CSS. A previous attempt to define services and roles was made in mid-2018, under the prior leadership at EIS and CSS. These efforts were ultimately scrapped and the new attempt with the vendor was done in 2020. As such, management turnover, as well as continued review by EIS management of staff knowledge, skills, and abilities, has delayed complete definition of the roles and responsibilities.

Risk and vulnerability management would be enhanced by robust enterprise-level monitoring and analysis

One of the key functions of security management is to identify and manage risk. This should be considered on both an organization-wide basis as well as an agency basis. This also includes mitigating identified vulnerabilities on a timely basis.

State statute requires agencies to conduct periodic information security assessments or to contract for assessments.[17] Agencies are also required to report the results of any vulnerability assessments, evaluations, or audits to EIS "for the purposes of consolidating statewide security reporting."[18]

The statewide security plan expands on these requirements by directing agencies to conduct risk assessments in accordance with best practices, including identifying, analyzing, and evaluating risks; identifying and evaluating options for the treatment of risk; and selecting control objectives and controls for the treatment of risks. It also requires agencies to establish an information security risk management framework to manage its risk program.

While these are important requirements for identifying and managing risk, there should also be enterprise-level procedures to manage and evaluate risks at the agencies, especially given the overall responsibility of the State CIO for information security in the executive department. However, there is currently no enterprise-level security risk management program to track whether risk assessments are occurring as required, to review or evaluate risks for the purposes of statewide security reporting, or to determine whether risks are being mitigated timely. EIS managers indicated they discuss risks being observed at agencies to potentially devise enterprise solutions, but without formal procedures, there is less assurance that all relevant risks are being identified and evaluated.

Statute also enables EIS to conduct vulnerability assessments of state agency information systems to evaluate and respond to the susceptibility of information systems to attack or disruption.[19] To support this requirement, several years ago CSS acquired and rolled out vulnerability scanning tools to agencies. As recently identified by CSS, almost 50% of agencies they have some

[17] ORS 276A.306(3)
[18] ORS 276A.300(8)(b)
[19] ORS 276A.300(3)(c)

responsibility for supporting are currently using this tool for internal vulnerability scanning. Among other responsibilities, CSS maintains the central vulnerability assessment tools, manages the associated contract and infrastructure, helps configure agency repositories and scan zones, establishes accounts for agency point-of-contact users, produces centralized reports to agency directors and CIOs, and produces an enterprise-level report to summarize activities across the enterprise. CSS also manages additional external scans conducted by the federal Cyber and Infrastructure Security Agency. Agencies are responsible to run their internal scans and address the vulnerabilities.

However, CSS does not directly track or assess whether agencies are remediating critical vulnerabilities timely. The enterprise-level CISO report provides a percentage of vulnerabilities that are more than 30, 60, or 90 days old, but this does not disclose what these vulnerabilities are or why they are not being mitigated. CSS is available to provide consulting services to agencies to assist in remediation if requested.

CSS recognizes the value of and need for enterprise-level cybersecurity risk and vulnerability management. However, management identified there are currently significant challenges in managing the risk program, and additional resources are required to improve the vulnerability management program.

Security risk and vulnerability management

Information security risk management is the process of managing risk associated with the use of information and information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of organizational assets, with the goal of addressing those risks in accordance with a clearly established organizational risk appetite and level of tolerance.

Vulnerability management is defined as the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, particularly in software.
- Source: EIS draft documents

For risk management, CSS identified current risk management and compliance tracking processes at agencies are very labor-intensive and scaling up to statewide oversight could quickly overwhelm the CSS risk management staff. In 2019, CSS began a project to procure an Enterprise Integrated Risk Management tool to provide enterprise-level risk management services. With this tool, they expect to provide a centralized repository for agencies to report security risks and track their resolution. This tool is intended to be a resource for agencies as well as for CSS to better track and review the status. Through leadership changes and challenges with procurement timelines, the tool was only procured on June 24, 2021. After procurement, significant additional work will be needed to set up and configure the tool, train staff at CSS, and roll out the tool to agencies in future biennia. Such efforts are likely to last at least through the end of the 2021-23 biennium, pending funding for ongoing efforts.

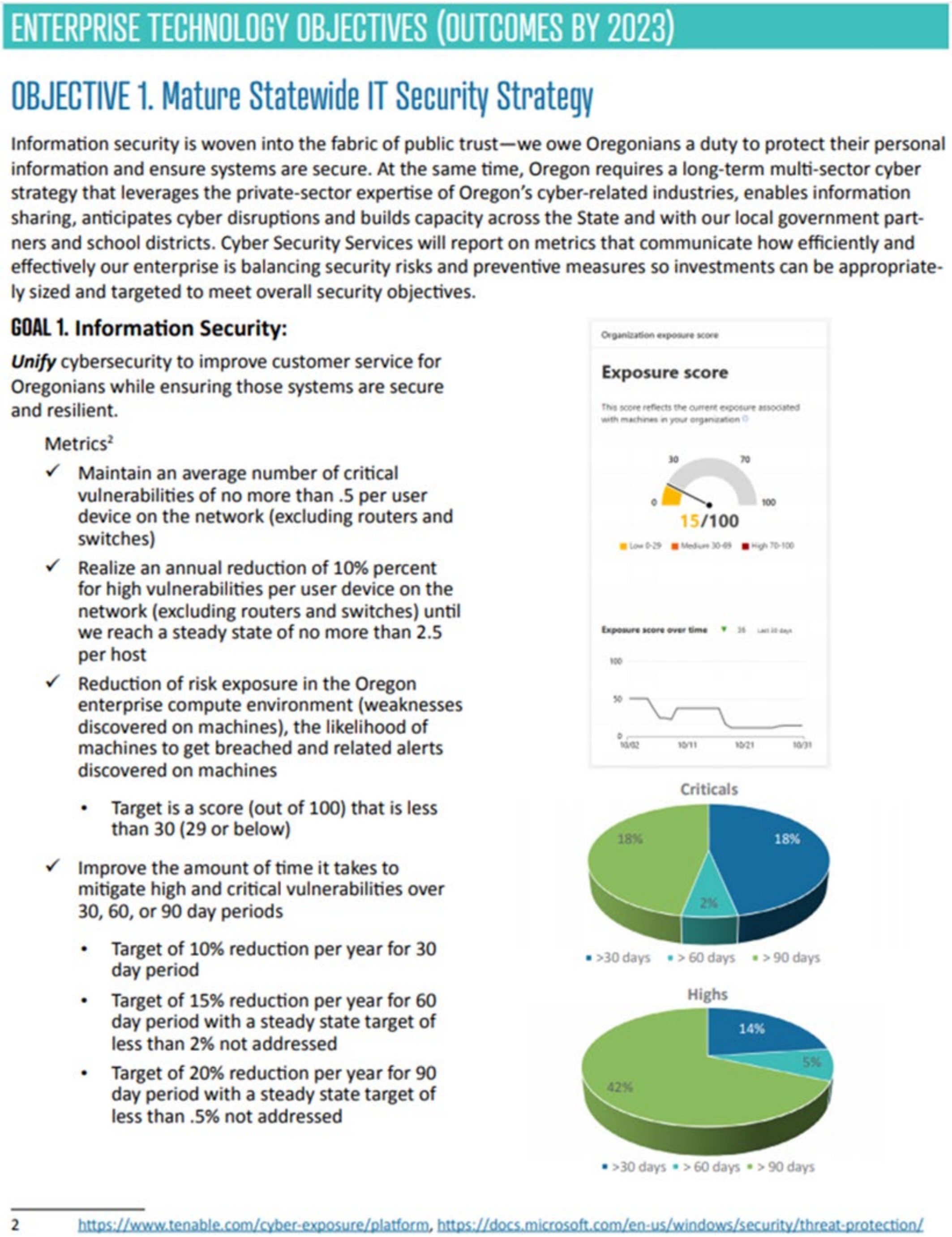
A recent assessment of CSS identified additional resources for vulnerability management are needed to improve and enhance the program. The budget request for 2021-23 included a policy option package requesting additional personnel to assist with remediating vulnerabilities at agencies, to expand the scope of scanning, and to increase capacity. The budget request, including the policy option package, was approved by the Oregon State Legislature and signed by the Governor on July 1, 2021.

Without centralized risk and vulnerability management the state runs the risk of having identified risks and vulnerabilities that are not being timely mitigated by agencies and that can affect the security posture of other state agencies. The state CISO also cannot obtain quality enterprise data on information security risk across agencies, which increases the difficulty of making decisions about how to best deploy state security resources.

IT security strategic planning should be enhanced

Leading practices indicate high-level strategic plans should be supported by additional tactical plans, or plans more specific to a particular area, such as IT security. This helps better define more short-term or specific initiatives or strategies to fulfill the goals or objectives in a high-level strategic plan.

Figure 7: Objective 1 in the EIS Strategic Framework, "Mature Statewide IT Security Strategy", does not define an end state



ENTERPRISE TECHNOLOGY OBJECTIVES (OUTCOMES BY 2023)

OBJECTIVE 1. Mature Statewide IT Security Strategy

Information security is woven into the fabric of public trust—we owe Oregonians a duty to protect their personal information and ensure systems are secure. At the same time, Oregon requires a long-term multi-sector cyber strategy that leverages the private-sector expertise of Oregon's cyber-related industries, enables information sharing, anticipates cyber disruptions and builds capacity across the State and with our local government partners and school districts. Cyber Security Services will report on metrics that communicate how efficiently and effectively our enterprise is balancing security risks and preventive measures so investments can be appropriately sized and targeted to meet overall security objectives.

GOAL 1. Information Security:

Unify cybersecurity to improve customer service for Oregonians while ensuring those systems are secure and resilient.

Metrics[2]

- ✓ Maintain an average number of critical vulnerabilities of no more than .5 per user device on the network (excluding routers and switches)
- ✓ Realize an annual reduction of 10% percent for high vulnerabilities per user device on the network (excluding routers and switches) until we reach a steady state of no more than 2.5 per host
- ✓ Reduction of risk exposure in the Oregon enterprise compute environment (weaknesses discovered on machines), the likelihood of machines to get breached and related alerts discovered on machines
  - Target is a score (out of 100) that is less than 30 (29 or below)
- ✓ Improve the amount of time it takes to mitigate high and critical vulnerabilities over 30, 60, or 90 day periods
  - Target of 10% reduction per year for 30 day period
  - Target of 15% reduction per year for 60 day period with a steady state target of less than 2% not addressed
  - Target of 20% reduction per year for 90 day period with a steady state target of less than .5% not addressed

Organization exposure score

Exposure score

This score reflects the current exposure associated with machines in your organization

[2] https://www.tenable.com/cyber-exposure/platform, https://docs.microsoft.com/en-us/windows/security/threat-protection/

Source: EIS Strategic Framework

For EIS, documentation is lacking as it relates to defining the forward-looking enterprise security strategy. The strategic planning document for EIS, the Strategic Framework, does not provide sufficient details regarding actual strategies to be followed in order to meet defined goals and objectives in the security section. The security-related objective is to "mature statewide IT security strategy" with a goal to "unify cybersecurity to improve customer service for Oregonians while ensuring systems are secure and resilient." The associated metrics address some aspects of ensuring systems are secure by measuring vulnerabilities and threats to computing resources as determined by monitoring tools.

However, this document does not define what IT security strategy maturity means, address how cybersecurity will be further unified, nor how in turn that will improve customer service and ensure systems are secure. While EIS has communicated some additional high-level initiatives to the Legislature, there are no formal supporting IT security-specific strategic or tactical plans, which would be better suited to providing this level of detail.

Lack of comprehensive strategic documentation does not mean that planning and activities to improve enterprise security are not occurring. The strategic framework includes an appendix showing overall EIS strategic project priorities through 2023. EIS also maintains an internal portfolio of projects that include additional efforts undertaken by various sections of EIS, including CSS. While detailed evaluation of these projects was not included in our audit scope, we noted several of them are intended to improve aspects of enterprise security. For example, the Network Security Modernization Program is in its early planning stages but is expected to eventually include projects to improve network resiliency and security. We reviewed selected business cases and noted they referred back to how the project supports the goals or objectives of the Strategic Framework or the Governor's Action Plan.

These multiple and disparate project documents do not provide a cohesive view of how these efforts are expected to improve or unify cybersecurity. Such documents also do not address non-project activities that may be taking place to enhance security services or to help address the goal and objective defined in the Strategic Framework. For example, they do not address an effort to modify the vulnerability measures to better reflect risks to systems as opposed to being solely compliance-based or the effort to refine the security service catalog and define publicly reportable metrics for all service lines. EIS managers acknowledged they could improve documentation of their plans for enhancing security but had ultimately prioritized work in other areas. For example, CSS provided pandemic support to help secure work from home and respond to a spike in threats, as well as support an accelerated migration and deployment of Microsoft 365 applications to over 40 agencies.

Defining lower-level goals, objectives, or tactics would help define the scope and end results of strategic efforts. Without cohesive or more detailed security strategic or tactical plans, there is not a complete definition of how different efforts tie together toward meeting an associated objective or goal. It also does not allow agencies sufficient information to know what EIS is planning to do to enhance security, which may affect their planning activities.

Key security management documents need to be updated

According to a DAS internal procedure, the division responsible for a policy will perform periodic reviews every two years to ensure policies comply with current law. This longstanding policy review timeframe is reiterated in the latest update to the statewide Cyber and Information Security policy as of November 2020. Per that addition to the policy, CSS will review the Statewide Information Security Plan, policies, and standards annually and update these documents, at a minimum, every two years.

Statewide IT Policies are outdated
Out of 12 statewide IT policies controlled by EIS, six are over 10 years old.

Yet several of the existing security management documents are significantly outdated. EIS controls 12 of the 14 statewide IT-related policies but has not updated or reviewed six of them in the last 10 years. A seventh policy is over eight years old. One of the policies includes a link to a web page that is intended to include several attachments, but the web page is not active.

Some documents on the EIS website are also outdated. For example, while the 2018 statewide security plan is included, there are also links to an older security plan template, and evaluation templates for agency security plans with the signature block of a state CISO who left state service in 2013.

In addition, there are some key areas addressed in the security plan where there are no associated policies to help further clarify expectations and roles and responsibilities between EIS and agencies. These include risk management, vulnerability management, security awareness training, mobile device management, and third-party relationships. The security plan itself is also three years old and still uses the pre-2020 names for EIS sections.

The fact that many of these policies are significantly out of date demonstrates EIS has struggled to update and maintain these policies over the last decade. Current leadership at EIS convened a new group in December 2019 to update the policies. The group updated three statewide policies in 2020 and work is ongoing to update additional policies. However, EIS has not yet developed a charter for this group to formally establish an ongoing role for it or any similar group. Establishing an ongoing process will help to ensure policies are proposed, reviewed, updated, and approved to ensure policies remain current and relevant.

Out-of-date documents, including those leading to broken web links, contribute to lack of confidence by customers that the policy statements still reflect current requirements or practices. It is also more difficult to ensure compliance with policies. In addition, lack of certain policies means additional details regarding roles and responsibilities between EIS and agencies are not available in those areas, potentially leading to misunderstandings regarding which entity is responsible for more detailed procedures.

EIS does not have robust mechanisms to ensure agencies are complying with rules, policies, and standards

Per statute, the State CIO is required to "assess state agencies each biennium to evaluate compliance with the State Chief Information Officer's rules, policies and standards and provide results of the assessments to the Governor and to the Joint Legislative Committee on Information Management and Technology."[20] This statute was passed into law in 2015, and the last report submitted to the committee was dated 2016.

Some of the services offered by CSS can help assess or track specific areas of compliance. For example, the security awareness training section tracks whether required annual training is occurring. In addition, BISOs use a spreadsheet to validate whether new IT investments are complying with statewide security standards. CSS also conducts security risk assessments of agencies to help them comply with the statutory requirement to obtain periodic information security assessments. However, checking compliance with rules, policies and standards is not the primary purpose of these assessments, and CSS lacks the resources to conduct these assessments each biennium for each agency.

[20] ORS276A.203(4)(a)(G)

Other than these services, EIS has not designed any specific procedures to evaluate agency compliance with rules, policies, and standards each biennium. The statewide Cyber and Information Security policy delegates responsibility to agency directors by indicating "each agency head is responsible for. . . ensuring the agency's compliance with the Statewide Information Security Plan, state policies, standards and initiatives, and with applicable federal and state law regulations." It also directs agencies to "implement policies and procedures to regularly monitor and assess their cyber and information security programs." However, there is currently no mechanism for agencies to report or attest to any compliance-related status to EIS for any kind of centralized reporting to the joint legislative committee.

Without ensuring compliance with rules, policies, and standards, the state does not have assurance that the important safeguards defined in those documents are being implemented as required at agencies. If safeguards are not applied uniformly, the state is at a higher risk that a vulnerability at one agency could negatively affect other agencies.

EIS should take action to improve coordination of communication efforts

When an entity has centralized authority, it should ensure services, roles and responsibilities, requirements, decisions, or pertinent information are appropriately communicated to customers, so everyone has an understanding. In addition, to ensure stakeholder engagement, there should be procedures to identify all relevant stakeholders and to group them into categories with similar information needs, then determine communication methods for each of these stakeholders. Procedures should also be established to periodically validate communication methods are effective and to determine whether adjustments should be made. More mature organizations should develop communication strategies or plans to ensure information is received and understood.

EIS sections have informally defined multiple external stakeholders, including agency directors, agency CIOs, information security personnel, DAS IT procurement, Legislative Fiscal Office analysts, and agency project managers. They have also identified multiple methods of communicating with these stakeholders, both formal and informal, to communicate information such as requirements, expectations, services, and roles and responsibilities, to the extent these have been completed. These methods include:

- Documents published on or linked from the EIS website, such as statewide policies, procedures, standards, plans, templates, and forms;
- Other information included on the EIS website, such as presentations and recordings of webinars;
- Presentations to and meetings with governance entities, specifically the ELT and the EITGC;
- Presentations to and meetings with other communities of interest, such as the CIO Council and Information Security Council;
- Public presentations to legislative committees, in particular the Joint Legislative Committee on Information Management and Technology;
- Emails to public GovDelivery communities of interest;[21]
- Emails to private listservs containing members of communities of interest, such as information security personnel and vulnerability management technicians;
- Policy area meetings with representatives from EIS and IT personnel from agencies, though these are not yet established for all policy areas;
- Live outreach events, such as webinars and forums;
- Newsletters, promotional materials, or handouts;

[21] https://public.govdelivery.com/accounts/ORDas/subscriber/new

- Other website tools, such as the IT Catalog for the BaseCamp program and datasets published on data.oregon.gov;
- Emails, phone conversations, in-person discussions, and other general communication methods used as part of ongoing business correspondence with peers and customers; and
- Information sharing by relevant EIS personnel while providing other IT services, such as Assistant State CIOs, Senior IT Portfolio Managers, BISOs, and the risk assessment team.

EIS also has several contact email addresses available on its website which are often included in email correspondence or at the end of presentations. EIS indicated these various addresses were monitored and the goal is to respond within 24 hours to requests or questions.

These methods are used as deemed relevant by managers of the EIS sections. One section has begun drafting a communication plan. However, there is no formal communications strategy that has been developed for individual sections or for EIS as a whole to help define what type of communication should be shared, to which stakeholder group, when, and by which methods. Private listservs are only informally shared and maintained. Several EIS managers also expressed a desire for a more defined communications process.

Overall, we concluded that EIS is sharing information to relevant stakeholders from each section and at the appropriate enterprise level, but lacks cohesion in its efforts to communicate expectations, requirements, services, and clear division of roles and responsibilities. Agency leaders recognize the need to establish clarity on those areas of communication.

Without formally defined communications strategies, EIS risks sharing information differently with different stakeholders and sharing information inconsistently. This is especially true since a large proportion of communication was reported to be informal, relating to conversations rather than presentations. This can lead to lack of common understanding of important expectations, requirements, or roles, as well as frustration on the part of customers who have not received the same communication as other customers or stakeholders.

Recommendations

To improve governance documentation and expand governance activities, we recommend EIS:

1. Develop new or update existing documents to describe the current governance structure and roles of subordinate enterprise IT governance groups in the executive department.

2. Establish and document an enterprise-level cybersecurity risk governance structure to establish risk management priorities, guide the risk management strategy, and define a minimum enterprise risk appetite.

To improve documentation of IT enterprise security management and to expand oversight, we recommend EIS:

3. Fully define the services CSS performs to provide enterprise-level support and security to agencies, including:

   a. Who provides the service;
   b. How customers should request the service; and
   c. How performance against that service is measured and reported.

4. Define clear divisions for assignment of "responsible" and "accountable" roles for capabilities listed in the CSS RACI chart when those assignments overlap.

5. Expand enterprise-level risk and vulnerability management programs to:

   a. Track whether assessments are occurring as required by statute and the statewide security plan;
   b. Assess and analyze risk or vulnerability patterns;
   c. Ensure risks and vulnerabilities are being timely remediated at agencies; and
   d. Inform key stakeholders of risks and mitigations.

6. Develop a more detailed IT security strategic plan to define specific and measurable goals for the enterprise security program.

7. Formally define a continuous process to propose, develop, evaluate and update required statewide IT policies, procedures, plans, and standards.

8. Develop processes to evaluate and report as to whether agencies are complying with key rules, policies, and standards.

To better utilize available communication channels, we recommend EIS:

9. Evaluate and update its website where applicable to ensure content is relevant and current.

10. Develop a communications strategy to document and describe how it communicates decisions, expectations, and roles and responsibilities to its customers, and how it ensures these communications are received and understood.

Objectives, Scope, and Methodology

Objectives

Determine whether Enterprise Information Services (EIS) has:

1. Developed and implemented an IT governance program for the oversight, integration, acquisition, development, planning, security, and use of executive branch agency information resources.
2. Designed and implemented controls to ensure effective management and oversight of executive branch IT security.
3. Defined, developed, and implemented effective processes to communicate enterprise-level expectations, requirements, services, and division of roles and responsibilities to executive branch agencies and other customers.

Scope

This audit focused on the EIS controls and processes pertaining to enterprise IT governance and enterprise IT security management, including evaluating whether they addressed selected responsibilities outlined in statute we deemed relevant to our audit objectives. We also identified the roles of higher-level governance groups not directly controlled by EIS to provide context. Auditors also assessed how expectations and requirements for agencies were documented and communicated. We also considered definitions of EIS services and how they are communicated, how they fit into overall enterprise IT security management, and how roles and responsibilities are defined and communicated.

We considered all sections within EIS except for Data Center Services and Data Governance and Transparency, as these sections have been the subject of recent or periodic audits. However, even for the sections in scope, we focused on functions not already covered by other recent audits. Additionally, areas out of scope for this audit were governance associated with Geographic Information Systems, State Interoperability, and Broadband services.

We focused on controls and processes as they exist during the audit period of 2020 through 2021, though we included some historical context extending back to 2019 and 2018, as relevant.

The following internal control principles were relevant to our audit objectives:[22]

- Control Environment
  - We considered whether management has established an organizational structure, assigned responsibility, and delegated authority to achieve the entity's objectives relevant to IT security management and oversight.
- Control Activities
  - We considered whether management has designed control activities to achieve objectives and respond to risks as it affects executive branch agencies.
  - We considered whether management implemented control activities through policies relevant to IT governance and security.

[22] Auditors relied on standards for internal controls from the U.S. Government Accountability Office, report GAO-14-704G.

- Information and Communication
    - We considered whether management externally communicated quality information to achieve the agency's objectives relevant to expectations, requirements, services, and roles and responsibilities.

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

Methodology

To gain an understanding of IT governance structures and roles, enterprise IT security management and oversight procedures, and communication methods, we conducted interviews with the following personnel:

- State CIO;
- Deputy State CIO;
- State CISO;
- Deputy State CISO;
- EIS Cybersecurity managers;
- EIS Shared Services, Strategy & Design, and Project Portfolio Performance managers;
- Chair of the EITGC; and
- Legislative Fiscal Office principal analyst.

We evaluated documentation relevant to our audit objectives, including:

- Governance diagrams, processes, and committee charters;
- IT strategic plans;
- Statewide IT security plans and standards;
- Statewide IT policies and procedures;
- CSS security catalog; and
- Description of roles and responsibilities.

Additionally, we performed a limited review of business cases for projects being led by EIS.

For our criteria, we used the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Special Publication 800-53 Rev 5, International Organization for Standardization (ISO) 27002:2013 5.1, the ISACA publication COBIT 2019 "Framework – Governance and Management Objectives," and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify best practices and controls deemed relevant to our audit objectives. We also referred to State of Oregon statutes and policies to determine EIS authority and responsibilities over IT governance and security.

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 courtesies and cooperation extended by officials and employees of EIS during the course of this audit.

Oregon

Kate Brown, Governor

Department of Administrative Services

Enterprise Information Services
155 Cottage Street NE
Salem, Oregon 97301

08/20/2021

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled *EIS Has Established an IT Governance Framework but Must Do More Regarding Cybersecurity Management*.

Enterprise Information Services (EIS) thanks the Secretary of State for performing this audit over the last 16 months. EIS provided hundreds of documents as evidence that delivery of several items associated with the scope of this audit is already in flight. We appreciate your partnership and thank you for recognizing where good work is already being done.

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

RECOMMENDATION 1 Develop new or update existing documents to describe the current governance structure and roles of subordinate enterprise IT governance groups in the executive department.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	March 2022	Joe Wells 971.707.0281

Narrative for Recommendation 1
Enterprise Information Services will update existing documents to reflect recent changes; however, given the time needed to establish new governing bodies, several updates may be required in order to reflect resolution of items associated with other recommendations in this audit.

RECOMMENDATION 2 Establish and document an enterprise-level cybersecurity risk governance structure to establish risk management priorities, guide the risk management strategy, and define a minimum enterprise risk appetite.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	July 2024 (in totality)	Kristine Cornett 503.949.4526

Narrative for Recommendation 2

Cyber Security Services (CSS) has drafted an enterprise cybersecurity risk management plan that proposes the establishment of an enterprise risk governance body, an enterprise governance structure, and supports establishing an enterprise risk appetite. CSS has recently procured an Integrated Risk Management (IRM) tool to utilize as a repository to help inform the governance body of enterprise risks, as well as risk and mitigation tracking. Purchase and Implementation of IRM will occur over multiple biennia with expected completion mid-23-25. With POP 126 (21-23), CSS will be hiring new Security Analysts to align with the six policy areas in an effort to enable a more proactive partnership and improve agency engagement and response.

RECOMMENDATION 3 Fully define the services CSS performs to provide enterprise-level support and security to agencies, including: a. Who provides the service; b. How customers should request the service; and c. How performance against that service is measured and reported.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Partially Agree	December 2022	Gary Johnson 503.437.3246

Narrative for Recommendation 3

a. In the first half of 2021, CSS published Service Catalog version one (1.0). A comprehensive revision is targeted for release in January 2022.
b. CSS will update existing documents to provide greater clarity around how agencies request service and is planning on utilizing an IT Service Management (ITSM) resource that EIS is actively working on implementing.
c. CSS regularly collects and distributes metrics on a quarterly interval and plans align our metrics against our service catalog in support of starting to develop service level agreements (SLA) by December of 2022.

RECOMMENDATION 4

Define clear divisions for assignment of "responsible" and "accountable" roles for capabilities listed in the CSS RACI chart when those assignments overlap.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	January 2022	Gary Johnson 503.437.3246

Narrative for Recommendation 4

CSS is actively working on maturing and further detailing our RACI chart to provide greater clarity.

RECOMMENDATION 5

Expand enterprise-level risk and vulnerability management programs to:

a. Track whether assessments are occurring as required by statute and the statewide security plan;
b. Assess and analyze risk or vulnerability patterns;
c. Ensure risks and vulnerabilities are being timely remediated at agencies; and
d. Inform key stakeholders of risks and mitigations.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Partially Agree	June 2023	Annalise Famiglietti 503.378.6568

Narrative for Recommendation 5

a. CSS currently tracks these manually. In the future, CSS will leverage the IRM platform for tracking and assessments. With the passing of POP 126 this biennium (21-23), we have hired three (3) new assessors to further assist in meeting statutory requirements.
b. CSS, through our cybersecurity assessment and Tenable vulnerability scanning reports, provides quarterly metrics on risk & vulnerability patterns to the enterprise.
c. CSS will monitor and track risks & vulnerabilities through the IRM effort, as well as leveraging the Tenable Security Center reports and eliminate the need for our current practice of manual tracking.
d. CSS DOES currently inform key stakeholders of vulnerabilities through the Tenable Security Center reports and the Vulnerability Management program reports. Additionally stakeholders are informed of risks through cybersecurity assessments (agency exit briefs, executive summaries & detailed reports).

<table>
<tr><td colspan="3"><b>RECOMMENDATION 6</b>
Develop a more detailed IT security strategic plan to define specific and measurable goals for the enterprise security program.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>December 2021</td><td>Gary Johnson
503.437.3246</td></tr>
</table>

Narrative for Recommendation 6
CSS is actively working on an effort to consolidate our vision and strategy documentation into one comprehensive plan.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 7</b>
Formally define a continuous process to propose, develop, evaluate and update required statewide IT policies, procedures, plans, and standards.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>March 2022</td><td>Joe Wells
971.707.0281</td></tr>
</table>

Narrative for Recommendation 7
Enterprise Information Services will update existing process to reflect the recommendation listed above.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 8</b>
Develop processes to evaluate and report as to whether agencies are complying with key rules, policies, and standards.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Disagree</td><td></td><td></td></tr>
</table>

Narrative for Recommendation 8
There needs to be clear understanding of what “key” refers to in this recommendation. The State of Oregon Executive Branch operates through a highly decentralized organization model. Information Technology is no exception. As such, enforcement /compliance may or may not be supported by statute. Compliance through partnerships in a “coalition of the willing” environment can be very effective, but typically has to be confirmed by internal or external audit. Motivation to be compliant may be minimal and/or difficult and repercussions for missing the mark nearly non-existent.

RECOMMENDATION 9
Evaluate and update its website where applicable to ensure content is relevant and current.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	December 2022	Joe Wells 971.707.0281

Narrative for Recommendation 9
Enterprise Information Services will have website updated as appropriate and will request ongoing resourcing to maintain content.

RECOMMENDATION 10
Develop a communications strategy to document and describe how it communicates decisions, expectations, and roles and responsibilities to its customers, and how it ensures these communications are received and understood.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Partially Agree	June 2022	Joe Wells 971.707.0281

Narrative for Recommendation 10
Enterprise Information Services thoughtfully communicates utilizing several vehicles and forums and to numerous agency groups and individual stakeholders, as noted in this audit. In regards to strategy, EIS will develop a high-level document describing an overall communication strategy; however, ensuring understanding is to ensure cognition, which EIS is incapable of performing as stated above.

Please contact Joe Wells at 971-707-0281 with any questions.

Sincerely,

Terrence Woods
State Chief Information Officer

Audit Team

Mary Wenger, CPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Erika Ungern, CISSP, CISA, Principal Auditor

Julie Moffenbier, M.Acc., Staff 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 elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits