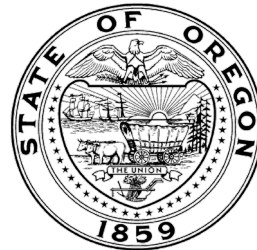


SECRETARY OF STATE

JLAC AUDIT BRIEFING



Department of Administrative Services and Enterprise Information Services:
EIS Has Established an IT Governance Framework but Must Do More Regarding
Cybersecurity Management

Report 2021-25, Released September 2021



AUDIT OBJECTIVES

Determine whether Enterprise Information Services (EIS) has:

1. Developed and implemented an information technology (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.



KEY FINDINGS

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

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.

3. Communications: EIS employs multiple communication channels but would benefit from definition of communication strategies.

IT Governance and Cybersecurity are Critical

Oregon cannot deliver public services effectively without effective IT governance and cybersecurity controls.

IT GOVERNANCE AND CYBERSECURITY MANAGEMENT ARE CRITICAL

- IT governance and cybersecurity management and oversight in the state of Oregon requires coordination and cooperation between many entities, including the Governor, 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.

EIS HAS SIX MAJOR PROGRAM AREAS

ENTERPRISE INFORMATION SERVICES

Cyber Security Services (CSS)

- Centralized security arm
- Encompasses governance, policy, procedure, and operations.

Project Portfolio Performance

- Oversees major IT investments
- Monitors adherence to policy and statute
- Provides training and tools to assist agencies

Shared Services

- Oversees several programs including E-Government, Quality Assurance, and Statewide Interoperability

Strategy & Design

- Contributes to enterprise strategic technology initiatives and technology standards, processes, and policy development

Data Governance and Transparency

- Charged with establishing Open Data standards and developing an enterprise data and information strategy.

Data Center Services

- Provides centralized computer services such as networking, email, backup, and server services

In Audit Scope Out of Audit Scope

GOVERNANCE IN OREGON

Governance consists of multiple layers and has multiple definitions. We defined the layers we deemed pertinent to Oregon and as it relates to EIS responsibility as Enterprise Governance and Enterprise IT Governance.

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.

GOVERNANCE IN OREGON

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.

ENTERPRISE IT PORTFOLIO

Focuses on evaluating proposed IT investments for alignment with enterprise 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 project.

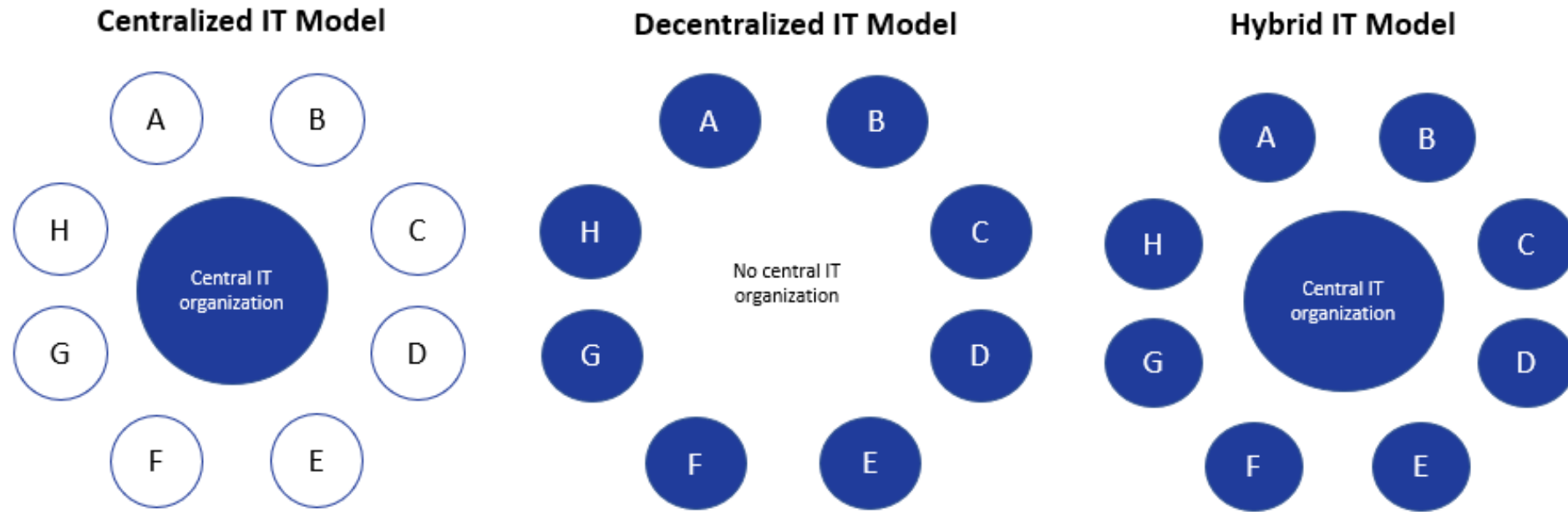
CYBERSECURITY

Ensures cybersecurity strategies support business objectives and helps reduce risks, formulate rules and procedures to help define expected best practices to follow, and assign responsibility for cybersecurity roles.

CYBERSECURITY RISK

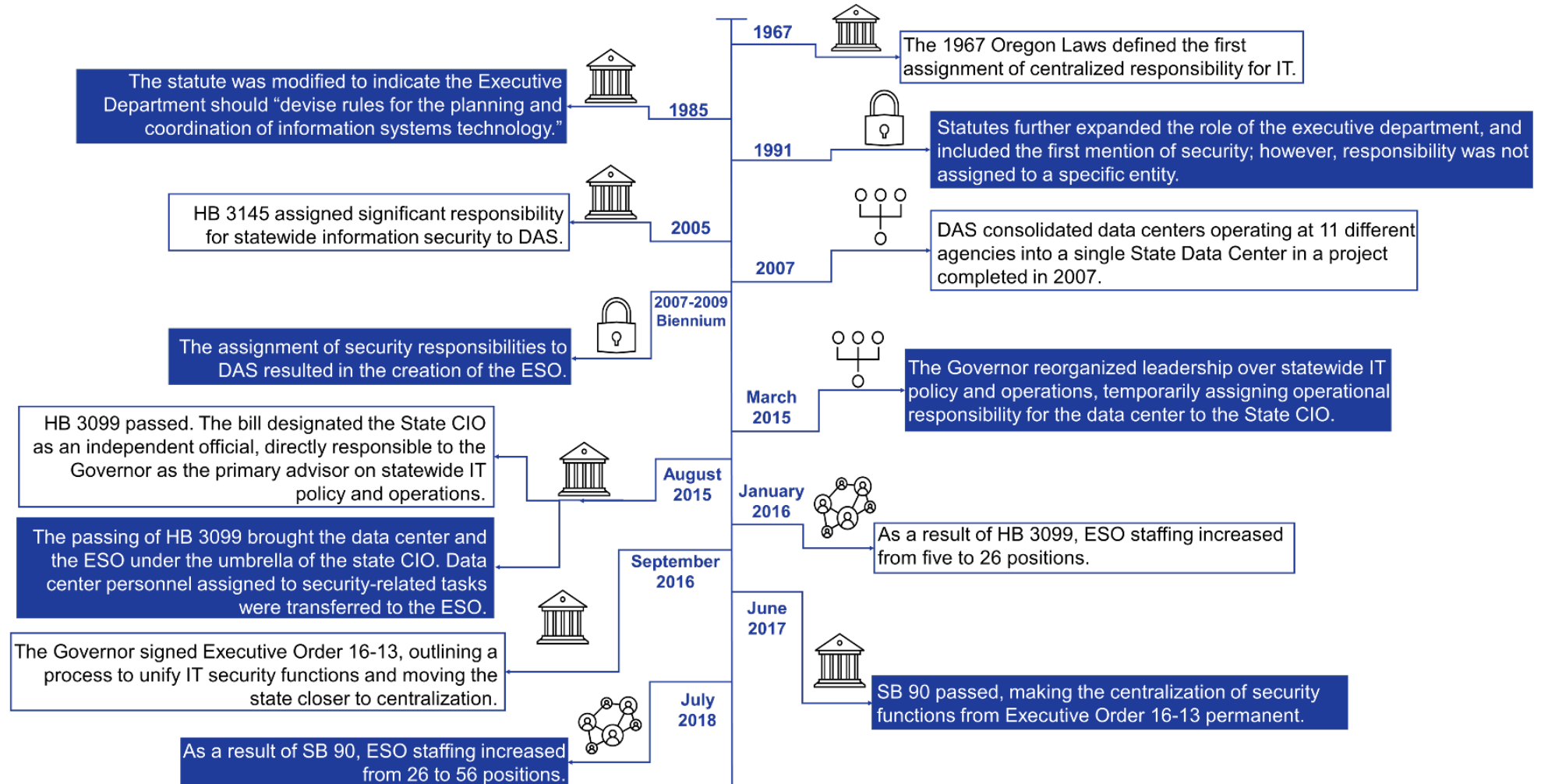
Help establish risk management priorities and guide the risk management strategy to ensure alignment with these priorities.

IT GOVERNANCE MODELS VARY



Blue Highlight: IT Governance and Resources
A-H: Business Units (Agencies)

IT GOVERNANCE AND OPERATIONS EVOLVE





AUDIT RESULTS – OBJECTIVE 1

IT Governance:

- 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.
- EIS develops or leads workgroups as needed to develop statewide IT policies, standards, or other documents for approval by the enterprise governance groups.
- Some supporting governance group definitions are outdated and should be clarified.
- 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.

RECOMMENDATIONS – OBJECTIVE 1

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.



AUDIT RESULTS – OBJECTIVE 2

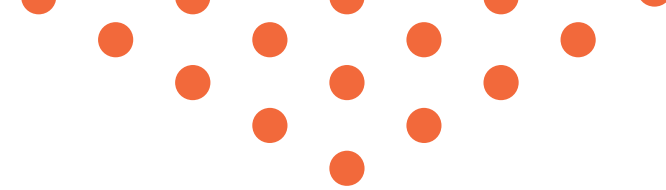
Cybersecurity Management:

- 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.
- EIS 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.
- IT security strategic planning should be enhanced.
- Some key security documents are outdated.
- EIS does not have robust mechanisms in place to ensure agencies are complying with rules, policies, and standards.

RECOMMENDATIONS – OBJECTIVE 2

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.
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.
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.



AUDIT RESULTS – OBJECTIVE 3

Communication:

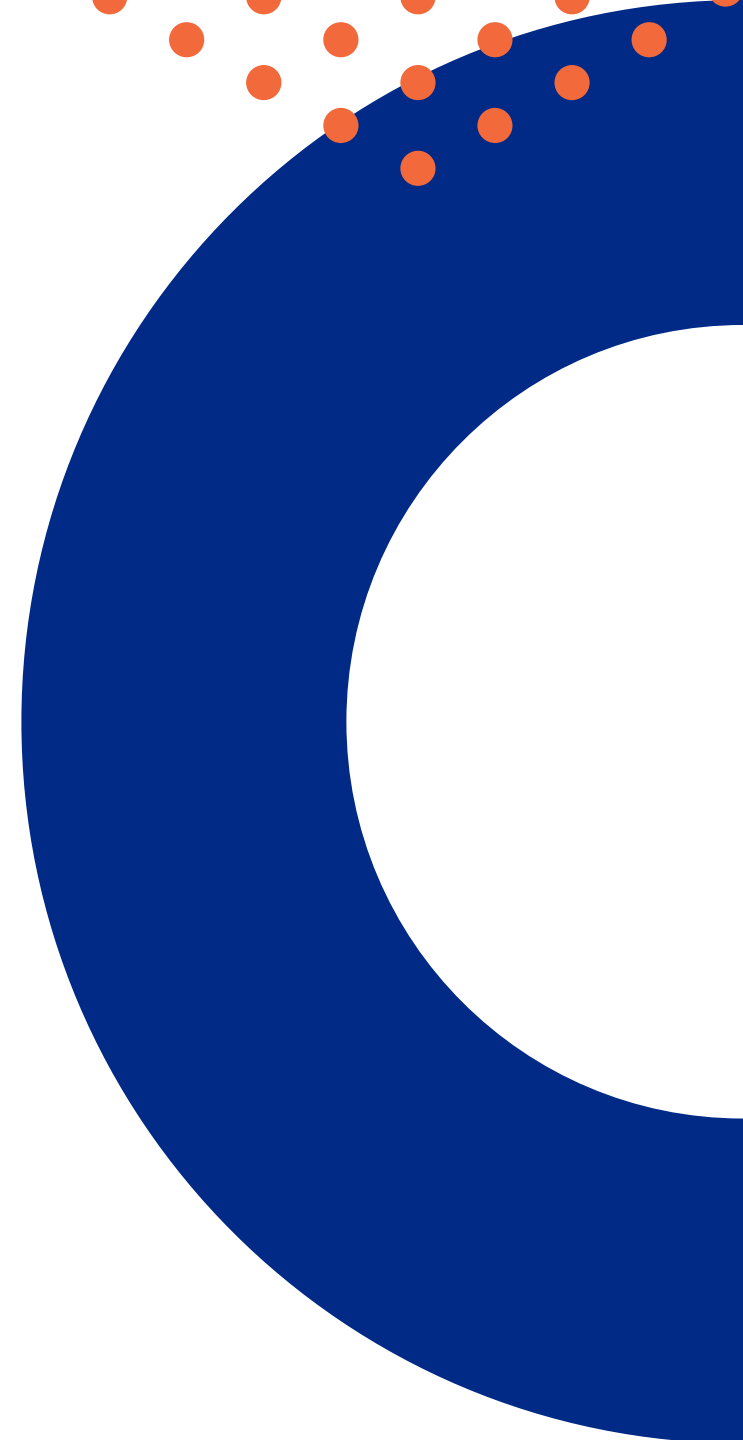
- EIS has developed multiple communication channels to inform agencies of needed information regarding EIS expectations, requirements, services, and roles and responsibilities.
- These communication efforts are largely ad hoc and would be enhanced by more formal procedures to define communication strategies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


RECOMMENDATIONS – OBJECTIVE 3

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.

QUESTIONS?





Teresa Furnish, IT Audit Manager
Audits Division, Oregon Secretary of State
teresa.l.furnish@sos.oregon.gov

Erika Ungern, Principal IT Auditor
Audits Division, Oregon Secretary of State
erika.a.ungern@sos.oregon.gov