ENTERPRISE
information services

Chief Technology Officer 2025-2027 Biennial Outlook

APRIL 2025

TABLE OF CONTENTS

TABLE OF FIGURES

1. Introduction

Enterprise Information Services (EIS) provides statewide information technology leadership through unification of Oregon IT policy and operations and specifically oversees state IT investments. Strategy and Design (S&D), as part of EIS, supports the mission by investing in and leveraging technology that transforms the way the state conducts business and the methods by which customers interact with state agencies. S&D empowers agencies to improve business performance and deliver a satisfying customer experience through secure innovative solutions and technology support offered from a statewide perspective.

The purpose of the State Chief Technology Officer's (CTO) Trends Outlook differs from ongoing program reporting on specific S&D initiatives. This outlook is intended to provide interested parties with insight into the thinking and priorities of the CTO, focusing on key emerging trends and the perspective of the CTO regarding the potential impact on Executive Branch service delivery, governance, and management in support of Oregonians.

The outlook shares the CTO's perspective on the key emerging business and technology trends that inform the priority of S&D's activities, initiatives, and projects in support of the Executive Branch:

- **Key emerging business trends**. These emerging business trends are expected to have a significant impact on state government in the foreseeable future. These trends are capable of changing how state workers interact with those seeking services.

- **Key emerging technologies**. These new technologies are currently being developed or are beginning to achieve practical application to state business processes. These technologies may be implemented in other sectors but may be largely unrealized within the state of Oregon. Emerging technologies are those that have the capability to change how services are delivered within the Executive Branch.

- **Technical debt**. These technical or organizational capabilities require significant maintenance effort but no longer fully support current business imperatives. These technologies or business processes must be modernized to meet the needs and expectations placed upon them.

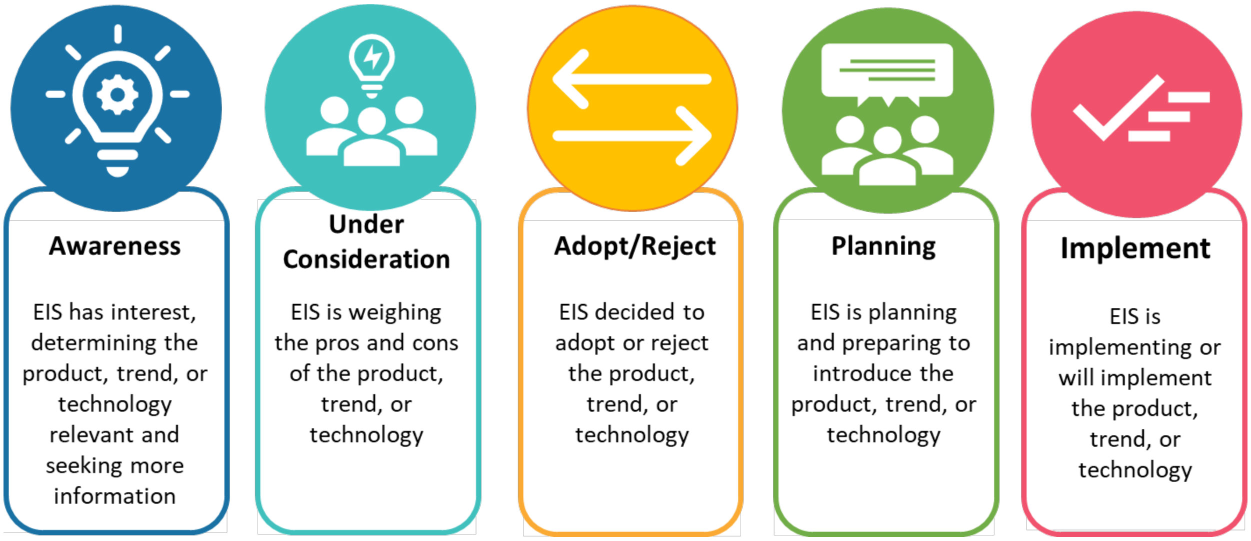
The trends outlook will evolve over time and will be influenced by budget, operational priorities, and strategic business objectives with a focus on positive outcomes for Oregonians

Though the primary purpose of this periodic document is not to provide detailed program reporting, it does demonstrate how emerging trends support the S&D program roadmap. S&D is charged with investing in and leveraging technology that will fundamentally transform the way the state conducts business and the methods by which customers interact with state agencies.

2. Key Emerging Trends

The following sections outline key emerging trends in business and technology that provide the context within which the Executive Branch operates. The trends are categorized by the current adoption level. Figure 1 (Adoption Level of Trends) describes the various adoption levels in more detail.

Figure 1: Adoption Level of Trends



Awareness

EIS has interest, determining the product, trend, or technology relevant and seeking more information

Under Consideration

EIS is weighing the pros and cons of the product, trend, or technology

Adopt/Reject

EIS decided to adopt or reject the product, trend, or technology

Planning

EIS is planning and preparing to introduce the product, trend, or technology

Implement

EIS is implementing or will implement the product, trend, or technology

The trend adoption levels are influenced by other processes such as the legislative budget planning, Enterprise Portfolio Governance, and Project Management Office processes.

2.1 Emerging Business Trends

The emerging business and technical trend analysis is strongly impacted by the following EIS published frameworks and strategies which help set the priorities and agenda for modernizing the enterprise infrastructure and governance:

- EIS Strategic Framework 2023-2026 Version 2.0
- Cloud Forward: A Framework for Embracing the Cloud in Oregon
- Oregon's Data Strategy: Unlocking Oregon's Potential
- Modernization Playbook: An Agency Guide to Digital Transformation – version 1.0
- Information Security Incident Response Plan

These business and technical trends are not exclusive to state government. Industries and organizations of all types are evaluating how to best manage both the potential and the risks to the workplace that these influential changes foreshadow.

Figure 2 (Key Emerging Business Trends) describes the trends and the CTO perspective with respect to the Oregon IT Enterprise. Each trend has an EIS evaluation icon to indicate where that trend is on the EIS adoption cycle. Each trend in the document is numbered for reference and traceability.

Figure 2: Key Emerging Business Trends

Business Trend	Description	CTO Perspective	EIS Evaluation	
			Prior	Current
Artificial Intelligence and Large Language Models 202503-B1	There are several places where Artificial Intelligence (AI) may come into play within the Oregon Enterprise. Some of these include Robotic Process Automation (RPA), Chatbots, or AI-driven eligibility. Additional uses include the ability to translate English pages on the fly and within cultural context or Low Code / No Code Software Development utilizing AI and RPA.	EIS is actively developing AI initiatives by fostering internal collaboration, improving AI usage tracking, and establishing an AI Operating Model with an approved framework. Currently conducting pilot projects, such as a CoPilot test environment and an EIS Policy Chat bot, while building resources and collaborating with external partners. Next steps include refining internal tracking and communication, forming AI workgroups, and continuing resource development. EIS calls for agency-wide participation in tracking AI work, contributing to AI framework development, and sharing policy expertise and resources to further strengthen their AI initiatives.	Awareness	Adopt
Customer Relationship Management 202503-B2	Customer Relationship Management (CRM), within a public sector context, is highly differentiated from private sector companies who use the processes for sales cycle, channel management and other revenue generation activities. In a government setting, Customer Relationship Management is the set of processes through which a public sector organization administers its interactions with citizens, businesses, and other interested parties. These processes support digital transformation to allow for citizen self-service, as well as call center and case management support.	Customer Relationship Management remains a key responsibility of most agencies. EIS has engaged in various discussions with partners and agencies to explore business cases, use cases, and potential tools such as CRM Software as a Service (SaaS) tool for reviewing.	Awareness	Under Consideration
Digital Government/Digital Services 202503-B3	Digital government and services include services such as digital signatures and licensing (including mobile driver licenses) as well as moving from physical to digital infrastructure. A key focus of digital government is to improve the citizen experience through digitization including additional	EIS intends to develop a citizen-centric IT architecture that promotes digital service delivery in an equitable and unbiased fashion in the following ways: • Support agencies with their digital service delivery efforts through consensus and coalition building. • Assist agencies to align future service offerings with best practices in human	Awareness	Awareness

Business Trend	Description	CTO Perspective	EIS Evaluation	
			Prior	Current
	online services and meetings, and digital assistants all while ensuring accessibility, proper identity management, and privacy protection.	centered design, customer experience (CX), and agile practices. • Embrace the need for CX and design thinking within the creation of digital public services.		
Data and Information Management 202503-B4	Data and Information management is a program that involves people, processes and technologies that provide control over the structure, processing, delivery, and usage of information assets. Information assets include both electronic and physical data and information in various formats and sources. Data and Information Management ensures that information is understandable, trusted, visible, accessible, and interoperable.	As Oregon's Data Strategy asserts, "Data is integral to all aspects of state government, from the administration and evaluation of programs, to funding and policy decisions." Oregon aims to ensure active data stewardship and governance so that data does not become a great user burden, or a harmful tool which codifies biased practices using low quality or decontextualized data. S&D actively supports the Chief Data Officer in building Oregon's capacity through people, processes, and technology to manage and utilize data strategically, establishing effective data governance, applying appropriate data justice frameworks, and building a culture of data literacy to transform data into meaningful insights. Through the Chief Data Officer, S&D is examining and evaluating "big data" toolsets to manage and analyze the data available in the state of Oregon.	⇆ Adopt	⇆ Adopt
Optimization 202503-B5	States are interested in optimizing information services, operations, resources, infrastructure, data centers, and communications platforms to allow Enterprise IT groups to simplify the environment while increasing capabilities and fostering "unified enterprise" thinking.	Digital transformation has resulted in the expectation that nearly every type of collaborative solution can be accessed through mobile devices with a single login, opening platforms across organizational boundaries. Integrated identity management, responsive websites, and mobile-driven experiences add layers of new application costs, security risks, and more complex technical support. EIS endeavors to provide agencies with a high-performance operating environment. Optimization is necessary to simplify our IT environments, reducing cost and risk while lowering the support cost of our increasingly technological environment.	Planning	Planning
Cloud Services 202503-B6	Cloud services encompass a variety of concerns including: • Cloud strategy • Selection of service and deployment models • Scalable and elastic services	To ensure sustained success and continuous improvement, EIS is driving this effort on multiple fronts: implementing the state's cloud strategy principles and establishing a Cloud Center of Innovation (CCoI) to actively encourage, educate, and empower	✓ Implement	✓ Implement

Business Trend	Description	CTO Perspective	EIS Evaluation	
			Prior	Current
	- Governance - Service management - Security - Privacy - Procurement	agencies in effective cloud utilization. This reflects our commitment to ongoing refinement and innovation and requiring no further updates to the established framework.		
Grant Management 202503-B7	Many agencies have expressed the need for a Grant Management Database Platform to streamline grant management processes. The platform will provide a single source of truth for all grant-related information, from application to closeout, while ensuring compliance with the latest Oregon laws and regulations.	EIS acknowledges the need for a Grant Management platform to be built on a scalable, cloud-native architecture with a focus on user experience and accessibility. Seamless integration with existing systems must be achieved through APIs, and robust security measures to protect sensitive data. A Grant Management platform will empower data-driven decision-making and free up valuable time for grant managers to focus on strategic initiatives.		Awareness
Case Management 202503-B8	A process-driven framework that manages transactions, services, inquiries, or responses, progressing through distinct phases from initiation to completion. This framework ensures the resolution of problems, claims, requests, proposals, developments, or other multifaceted activities over a defined timeline.	Case management should be integral to managing agencies transactions and requests, ensuring alignment with broader IT governance and strategic goals such as service excellence, transparency, and modernization.		Awareness
EIS Enterprise Architecture 202503-B9	Enterprise Architecture is a framework for developing and managing architecture that is flexible and focused on delivering value quickly and continuously. Strategy and Design will foster collaboration and communication, breaking down silos and promoting a shared understanding of our technological landscape and objectives.	The push for agency modernization has resulted in, and will continue to drive, the widespread adoption of new technologies. Implementing Enterprise Architecture (EA) in this context provides a structured approach to managing change, ensuring that modernization efforts are strategic and aligned with organizational goals.		Under Consideration
EIS Enterprise Architecture Review Board 202503-B10	The architecture review board (ARB) will help navigate the complexities of technological transformation, promoting a more cohesive, efficient, and strategically aligned approach to modernization efforts. The ARB is a governance body that will assess, evaluate, approve, or reject architectural designs to	As agencies embark on modernization initiatives that introduce new technologies, the Architecture Review Board (ARB) will play a crucial governance role for evaluating and approving architectural designs for new projects and significant changes; sustain the enterprise architecture's integrity, maintaining consistency and coherence across various technological		Under Consideration

Business Trend	Description	CTO Perspective	EIS Evaluation	
			Prior	Current
	ensure they align with business and technological goals.	implementations; enforce architectural standards and policies, promoting best practices and ensuring that all technology-related decisions support the agency's long-term goals.		
Identity Access Management 202503-B11	In today's hybrid work environment, the conventional corporate network perimeter has become less relevant as a primary security focus. Instead, Identity and Access Management (IAM) has emerged as the cornerstone of security in our increasingly interconnected world. Identity Access Management (IAM) is a security, a technology, and a business discipline to manage and secure digital identities and control user access to critical information.	By centering security around identity verification and access control rather than network boundaries, IAM will allow EIS to maintain robust protection regardless of where users are located or what devices they use. CTO objective would be business enablement through refined technology that meets security objectives. This strategy enhances overall security posture by ensuring that access is granted based on verified identity and need, rather than assumed trust within a network perimeter.		Under Consideration
Next-Generation IT Systems 202503-B12	Next-generation IT systems refer to advanced technologies and methodologies, such as low-code/no-code platforms, cloud-native applications, and agile development frameworks, designed to streamline and accelerate IT processes.	Next-generation IT systems can support in modernizing legacy platforms, improving citizen-facing services, and achieving digital transformation. By adopting agile methodologies and leveraging cloud-native tools, the state can reduce development timelines, and ensure secure, and accessible IT solutions that align with Oregon's strategic goals.		Awareness
Emerging Technologies for Targeted Applications 202503-B13	Emerging technologies for targeted applications focus on specialized solutions to address specific challenges, such as spatial computing for urban planning and disaster response, or AI for fraud detection and predictive analytics.	These technologies present opportunities to enhance public services by providing innovative tools for areas like environmental monitoring, transportation, and public safety. State of Oregon can deploy these technologies to optimize operations, improve decision-making, and address unique state-level challenges.		Awareness
Application / Licensing / Permitting 202503-B14	A system that assists external organizations or individuals applying or requesting approval, authorization or resources, and agencies with issuing, tracking, and renewing permits, licenses for regulated activities.	S&D acknowledges the need for application, licensing, and permitting system, emphasizing user-centric design. The platform would automate workflows and provide intuitive tools for both Oregonians and agencies.		Awareness
Telephony Contact Center 202503-B15	A telephony contact center initiative focuses on procuring alternate contact center solutions and managed service providers to enhance operational efficiency. It	The telephony contact center initiative represents a strategic opportunity to modernize and streamline communication infrastructure. The focus on procuring alternate solutions and		Awareness

Business Trend	Description	CTO Perspective	EIS Evaluation	
			Prior	Current
	aims to ensure a consistent experience for agencies when submitting service and incident tickets. Additionally, vendors will integrate seamlessly with the Shared Services' existing ticketing system to provide a streamlined and unified service management approach.	managed service providers aligns with the goal of enhancing scalability, reliability, and efficiency across the enterprise. Ensuring a consistent experience for agencies when handling service and incident tickets reflects a commitment to user-centric design and operational excellence.		
Application Portfolio Management 202503-B17	Application Portfolio Management (APM) is a strategic approach that empowers agencies to optimize their application portfolio by identifying redundancies, outdated software, and applications misaligned with business objectives.	APM is a critical tool for driving digital transformation. It provides a structured framework to assess and address technical debt, enhance resource allocation, and prioritize investments in modernization. By leveraging data-driven insights, APM supports informed decision-making, reduces costs, and ensures that the technology ecosystem is future-proof, agile, and aligned with strategic goals.		Awareness

2.2 Key Emerging Technologies

Figure 3 (Key Emerging Technologies) describes the emerging technology trends and the CTO perspective with respect to the Oregon IT Enterprise. Additionally, the icon with each topic indicates where that trend is on the EIS adoption cycle. The icons indicate the likelihood that EIS will incorporate these trends into the larger technology strategy framework, as well as the supporting guidance, plans and roadmaps. Note, this section does not make any recommendations regarding specific products.

Figure 3: Key Emerging Technologies

Technology Trend	Description	CTO Perspective	EIS Adoption	
			Prior	Current
Zero-trust security 202406-T1	Zero trust operates on the principle of “never trust, always verify”. This approach reduces the chances of unauthorized access because it doesn’t implicitly trust any user or device based on network location. Based on the principle that no user, device, or application can be trusted by default, this security framework has seen rapid adoption. Unlike VPNs, which mainly authenticate users at the initial	While there are many benefits to the zero-trust framework, there are also several challenges to be understood. Currently, most zero trust networks are designed to secure remote workers, automatically disabling themselves whenever the user logs in through the internal office environment. There are also legacy application and network topology considerations to be resolved. EIS will continue to explore the best use of a zero-trust networking approach.	Planning	Planning

Technology Trend	Description	CTO Perspective	EIS Adoption	
			Prior	Current
	connection, zero trust network access continuously evaluates the trustworthiness of a connection, considering factors like device health, user behavior, and context.			
Multi-cloud Access 202406-T2	Multi-cloud is the use of multiple cloud computing services from different cloud providers in a single heterogeneous architecture.	EIS is working on multi-cloud strategies to avoid vendor lock-in, increase resilience, optimize performance, and take advantage of the best services each cloud provider may offer our agencies. Our architecture will include services from AWS, and Microsoft Azure. We will evaluate Google Cloud Platform, and other specialized cloud providers as necessary.	Planning	Planning
Network Segmentation 202406-T3	EIS will review Network segmentation, dividing the network into smaller, distinct subnetworks, or segments, each of which to be managed and accessed separately.	EIS will enhance the security posture of the network, improves performance, and simplifies compliance management by isolating sensitive data and critical systems.	Planning	Planning
Software Defined Networking (SDN) Overlay 202406-T4	Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on the network.	EIS will utilize SDN overlay as a virtual network built on top of the Data Center existing physical network infrastructure, leveraging SDN principles to provide flexible, scalable, and enhance network performance.	Planning	Planning
Cloud Access Security Broker 202406-T5	Cloud Access Security Brokers (CASBs) are security policy enforcement points positioned between our users and cloud service providers to provide visibility, compliance, data security, and threat protection.	EIS will use CASBs to extend security controls to the cloud, maintain data security policies are consistently applied across on-premises and cloud environment	Planning	Planning
Network Access Control 202406-T6	EIS will use Network Access Control (NAC) to manage and enforce policies for accessing the network.	NAC ensures that only authorized users and compliant devices can connect to the network, thereby enhancing security and mitigating risks associated with unauthorized access and non-compliant devices.	Planning	Planning

Technology Trend	Description	CTO Perspective	EIS Adoption	
			Prior	Current
Microsoft Copilots 202406-T7	There are several places where Artificial Intelligence (AI) may come into play within the Oregon Enterprise. Some of these include Microsoft Copilots.	EIS is reviewing Microsoft Copilots for adoption. There is not a one size policy which covers all use cases for Copilots. EIS will soon provide additional interim guidance for the Executive Branch use of AI technology in compliance with the State Government Artificial Intelligence Advisory Council final action plan as required by Executive Order 23-26.	Awareness	Under Consideration
Microsoft Entra External ID for Customers 202406-T8	Microsoft Entra External ID for Customers is an element of Customer Identity and Access Management (CIAM), designed to enhance identity solutions for agencies. It provides seamless self-service registration capabilities for public-facing applications, empowering users to easily manage their access.	Microsoft Entra External ID for Customers is a strategic solution for advancing digital transformation and improving customer engagement. Its self-service registration feature minimizes administrative overhead while increasing user autonomy and satisfaction. The personalized sign-in experience enhances security and streamlines access, aligning with modern customer expectations.	Awareness	Awareness
Enhance SOC/NOC 202503-T9	The NOC (Network Operations Center) and SOC (Security Operations Center) are critical components of our IT infrastructure, with the NOC focused on maintaining network performance and availability, while the SOC is responsible for detecting and responding to cybersecurity threats.	Our Security and NOC capabilities has a three-pronged approach. Firstly, mitigate risks associated with security breaches and network disruptions, minimizing service interruptions. Secondly, boost resilience by pooling resources and sharing services and capabilities, allowing for a more robust and responsive infrastructure. Finally, establish a centralized Fusion Center for Network and Security Operations (FuNSOC) to streamline operations and improve coordination between security and network teams. This FuNSOC will act as a central hub for monitoring, managing, and responding to security and network events.		Under Consideration
Enhance Wi-Fi 202503-T10	Enhanced Wi-Fi refers to improvements made to a wireless network to provide better coverage, faster speeds, increased reliability, and stronger security. The goal of enhanced Wi-Fi is to create a seamless and positive user experience with strong connectivity, no matter where users are located within the network's range.	EIS will optimize Wi-Fi services across all Executive agencies by standardizing capabilities and improving user experience. This includes providing pervasive Wi-Fi coverage in all state buildings and offices, ensuring consistent service delivery, and implementing secure access protocols. By standardizing and enhancing Wi-Fi services, EIS seeks to create a seamless and reliable user experience for everyone.		Under Consideration
SD-WAN 202503-T11	SD-WAN or Software-Defined Wide Area Network, is a modern networking technology that allows connectivity among various locations (offices, data centers, cloud services) using any type of	EIS is pursuing the optimization of SD-WAN capabilities to achieve several key objectives. Primarily, we aim to standardize SD-WAN services across all remote branch offices, ensuring consistency and efficiency. This initiative includes		Under Consideration

Technology Trend	Description	CTO Perspective	EIS Adoption	
			Prior	Current
	internet connection. It intelligently prioritizes traffic, ensuring performance for critical applications, and often includes built-in security features.	enhancing SD-WAN's overall capabilities, focusing on improved service resiliency and failover mechanisms to minimize downtime. Additionally, we seek to reduce latency and optimize bandwidth by minimizing backhauling of cloud application traffic. Security is also a priority, with plans to integrate advanced security functions into the SD-WAN framework. Finally, we aim to streamline operations by automating service delivery and implementing comprehensive monitoring capabilities.		

2.3 Technical and Organizational Debt

The classic definition of technical debt is the cost of maintaining outdated systems as opposed to investing in better, newer solutions. When it comes to data centers, technical debt can refer to the usage of outdated infrastructure and hardware systems that reduce data center efficiency. This type of debt accumulates over time when data centers keep legacy systems in place as opposed to investing in new and improved technologies.

The term “organizational debt” was originally used by the entrepreneur Steve Blank, who defined it as the collection of changes that should have been made by an organization but weren’t. The phrase was a twist on the term “technical debt” which describes the accumulated cost of taking shortcuts when developing a technology or digital product. In both cases, the debt comes from making a choice with a short-term gain and a long-term compounding cost.

Both types of debt occur naturally in the rapidly evolving environment of technical advances and increased expectations of Oregonians and staff. Mainframes have been replaced by midrange servers, which have been replaced by cloud. Waiting in line to renew a driver’s license paid for by check has been replaced by a secure portal interaction with instant electronic payment. Technical and Organizational debt are not indicators of failure but of change.

That said, debt still requires assessment and action, because the “interest” on the debt compounds over time. Left unaddressed, the cost of doing nothing becomes significantly higher. Figure 4 (Debt Management Process) shows a classic style of managing technical and organizational debt.

Technical and organizational debt management have a lot of similarity with traditional risk management in that an analysis must be made to determine the cost of correction versus the benefit achieved. This must be balanced with other priorities and available resources and funding.

Figure 4: Debt Management Process

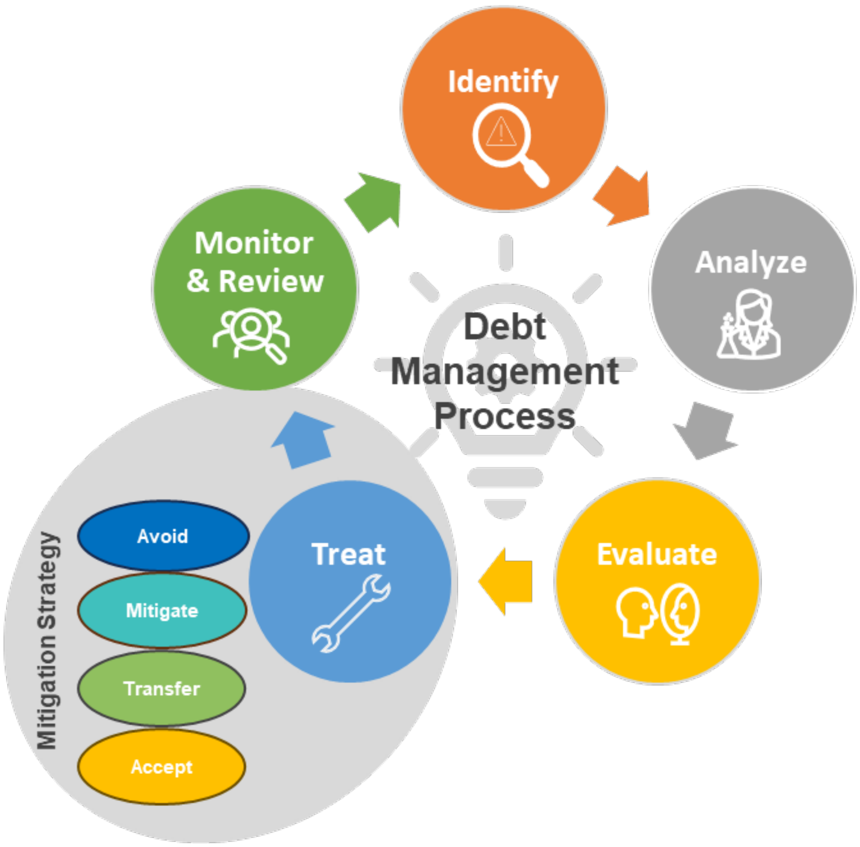


Figure 5 (Debt Management Process Steps) provides a description of the debt management process steps.

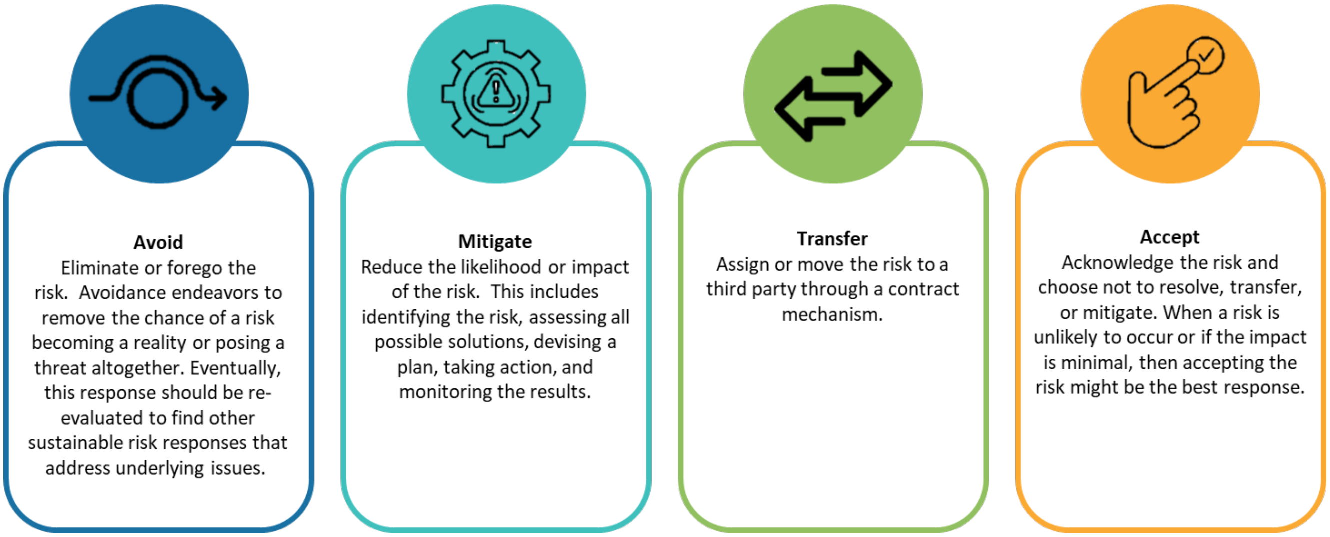
Figure 5: Debt Management Process Steps

Icon	Step	Description
🔍	Identify	Identify potential areas where technical or organizational debt is presented.
👤	Analyze	Analyze the quantitative debt and the rate of change.
🗣	Evaluate	Evaluate the potential impact and likelihood of occurrence. Create a debt management plan.

Icon	Step	Description
	Treat	Choose an alternative to address the debt. Prioritize the debt with the highest cost or greatest chance of failure.
	Monitor and Review	Monitor and review debt, making sure they are consistently identified and managed.

Once a decision has been made to address or treat the risks from technical or organizational debt, there are several possible approaches which can be taken. Figure 6 (Approach Descriptions) describes these approaches.

Figure 6: Approach Descriptions



Avoid
Eliminate or forego the risk. Avoidance endeavors to remove the chance of a risk becoming a reality or posing a threat altogether. Eventually, this response should be re-evaluated to find other sustainable risk responses that address underlying issues.

Mitigate
Reduce the likelihood or impact of the risk. This includes identifying the risk, assessing all possible solutions, devising a plan, taking action, and monitoring the results.

Transfer
Assign or move the risk to a third party through a contract mechanism.

Accept
Acknowledge the risk and choose not to resolve, transfer, or mitigate. When a risk is unlikely to occur or if the impact is minimal, then accepting the risk might be the best response.

Figure 7 (Technical and Organizational Debt and Risk Profile) describes the technical or organizational debt and the CTO perspective with respect to the Oregon IT Enterprise. Additionally, each debt area contains an EIS risk strategy description to indicate how EIS intends to address this debt. Each type of debt is classified by debt type, description, and approach to addressing the debt.

Figure 7: Technical and Organizational Debt and Risk Profile

Debt Area	Debt Type	Description	Approach		Mitigation Strategy
			Prior	Current	
Network Infrastructure 202406-D1	Technical	Aging infrastructure, resiliency, etc.	Mitigate	Mitigate	Enterprise Information Services contracted for a Network and Security Modernization Plan (NSMP) Roadmap in 2023. The roadmap is designed to result in a reliable, secure, and scalable foundation in support of business functions and modernization initiatives for all state agencies and their customers. The future state network and security infrastructure are expected to deliver comprehensive and integrated capabilities.
Legacy Moder-nization 202406-D2	Technical / Organizational	IT modernization of legacy systems in Oregon has been a critical issue for several years. Agencies have been modernizing their services and systems for more than a decade through large projects, but the level of technical debt is still considerable.	Mitigate	Mitigate	In support of the 2023-2026 EIS Strategic Framework Objective, “Mature Legacy System Modernization Strategies”, S&D is: • Working closely with the Assistant State Chief Information Officers (ASCIOs) to align agency modernization projects at the enterprise level. • Partnering with Project Portfolio Performance (P3) to ensure new projects minimize technical debt into the environment. • Evaluating application modernization services approaches including the migration from mainframe and on-premise servers into the cloud.
Organizational Change Management 202406-D4	Organizational	Recognizing the need for responsive leadership, clear purpose and priorities, quality communication, support for change and coordination in delivery	Mitigate	Mitigate	Transitioning to an “as a service” delivery mode requires a fundamental shift both with contracting and business operations. Contracts must clearly identify responsibility, service levels, security requirements, training expectations and risks. EIS is working with the agencies to evolve their contracting and operational expectations to address the necessary Organizational Change Management.

Debt Area	Debt Type	Description	Approach		Mitigation Strategy
			Prior	Current	
Governance 202406-D5	Organizational	The quickly evolving solution transition to a cloud forward strategy, coupled with contracting with multiple vendors and SaaS platforms across the agencies calls for a more rigorous architectural governance methodology.	Mitigate	Mitigate	EIS is establishing an Architectural Review Board (ARB) based in The Open Group Architecture Framework (TOGAF) to oversee IT investments from a program, project management and architectural perspective. The ARB provides a forum for decision making and the publication and enforcement of those decisions. Where appropriate, new policies, standards, guidelines, and procedures will be developed.

3. Summary

Oregon’s Enterprise Information Services (EIS) is driving modernization through key business and technology trends while fostering collaboration and communication with State agencies and interested parties to support the state’s vision of accessible, reliable, and secure technology systems for all Oregonians.

Business trends may potentially transform public service delivery through digital government initiatives, enhanced customer relationship management (CRM), data-driven governance, and modernized case management systems.

Technology trends emphasize innovation and security with solutions like zero-trust frameworks, multicloud strategies, network segmentation, and software-defined networking (SDN). Emerging technologies such as AI-powered tools, advanced automation, and enhanced Wi-Fi are central to building a resilient, efficient, and future-ready IT environment.

The CTO’s leadership will enhance communication and partnerships by establishing governance structures like the Architecture Review Board, fostering collaboration among policy areas, and aligning modernization efforts with shared goals. We will support agencies with strategic guidance, transparent decision-making, and tailored resources, ensuring the integration of business and technology priorities to serve Oregonians.

Our vision remains: to ensure accessible, reliable, and secure state technology systems that equitably serve all Oregonians. As we continue our focus on process improvement, we are strengthening governance and use frameworks to support our agencies in their modernization journey. Real change is driven by the dedication and efforts of our agencies, and we are committed to partnering with them to meet the needs of the Oregon public.