ENTERPRISE
information services

# Chief Technology Officer
# Introductory Quarterly Outlook

JUNE 2024

# 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) Quarterly Outlook differs from ongoing program reporting on specific S&D initiatives. This outlook is intended to provide stakeholders 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.

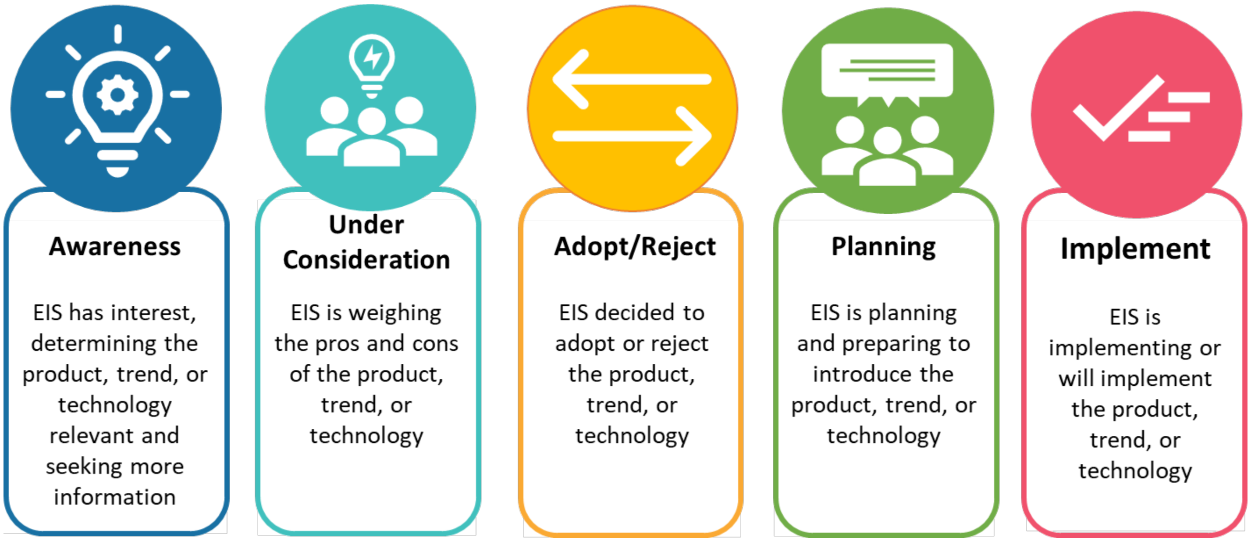
This quarterly outlook will appropriately evolve over time and will be influenced by budget, operational priorities, and strategic business objectives with an eye on positive outcomes for Oregonians.

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 |
|---|---|---|---|
| **Artificial Intelligence and Large Language Models**<br>202406-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. | Artificial Intelligence is a continuum of capabilities ranging from prewritten business rules to RPA to machine learning to generative AI. There is not a one size policy which covers all use cases.<br>Oregon executive leadership is providing interim guidance (link to State CIOmemo) for the Executive Branch use of AI technology while the State Government Artificial Intelligence Advisory Council completes a final recommended action plan as required by Executive Order 23-26. | Awareness |
| **Customer Relationship Management**<br>202406-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 stakeholders. These processes support digital transformation to allow for citizen self- | Customer Relationship Management is a key responsibility of nearly every agency. Agencies are coming to EIS for help in evaluating CRM tools. Many of these tools have been expanded to include configurable platforms to facilitate process automation and are now increasingly incorporating AI and other emerging technology to automate citizen interactions and reduce administrative burden and complexity of service delivery.<br>EIS is working to streamline the assessment and procurement of CRM Software as a Service tools to make the agency acquisition journey easier. This includes the reuse of product comparison evaluations from other agencies | Awareness |

| Business Trend | Description | CTO Perspective | EIS Evaluation |
|---|---|---|---|
| | service, as well as call center and case management support. | as well as the development over time of a preferred solutions catalog that agencies can take advantage of. | |
| **Digital Government/ Digital Services**<br>202406-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 customer experience through digitization including additional online services and meetings, and digital assistants all while ensuring accessibility, proper identity management, and privacy protection. | EIS intends to develop a customer-centric IT architecture that promotes digital service delivery in an equitable and unbiased fashion in the following ways:<br>• Support agencies with their digital service delivery efforts through consensus and coalition building.<br>• Assist agencies to align future service offerings with best practices in human centered design, customer experience (CX), and agile practices.<br>• Embrace the need for CX and design thinking within the creation of digital public services. | 💡<br>Awareness |
| **Data and Information Management**<br>202406-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, | 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.<br>EIS actively supports the Chief Data Officer in building Oregon's capacity through people, processes, and technology to manage and utilize data | ⇆<br>Adopt |

| Business Trend | Description | CTO Perspective | EIS Evaluation |
|---|---|---|---|
|  | visible, accessible, and interoperable. | strategically, establishing effective data governance, applying appropriate data justice frameworks, and building a culture of data literacy to transform data into meaningful insights.<br>Through the Chief Data Officer, EIS is examining and evaluating “big data” toolsets to manage and analyze the data available in the state of Oregon. |  |
| **Consolidation/ Optimization**<br>202406-B5 | States are interested in consolidating and 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.<br>Consolidation and optimization are necessary and effective tools to simplify our IT environments, reducing cost and risk while lowering the support cost of our increasingly technological environment. | Planning |
| **Cloud Services** | Cloud services encompass a variety of concerns including:<br>• Cloud strategy<br>• Selection of service and | Oregon has adopted a Cloud Forward Framework that envisions conducting 75% of its business via cloud-based services and infrastructure by 2025. This is a big transformation over a | Implement |

| Business Trend | Description | CTO Perspective | EIS Evaluation |
|---|---|---|---|
| 202406-B6 | deployment models<br>• Scalable and elastic services<br>• Governance<br>• Service management<br>• Security<br>• Privacy<br>• Procurement | limited timeframe.  EIS is approaching this effort on several fronts including the following:<br>• Implementing the state's cloud strategy principles to facilitate upskilling and successful adoption across the Oregon enterprise.<br>• Established a Cloud Center of Innovation (CCoI) to actively encourage and educate agencies in successful cloud utilization. | |
| **Continuing Expansion of Broadband**<br>20406-B7 | With the Federal Government releasing more than $42 billion in new funding to expand high-speed internet action nationwide, over 8.5 million families and small businesses will be able to take advantage of modern-day connectivity that is required at a level like electricity. | Within Oregon, the plan for broadband access and digital equity, administered by the Oregon Broadband Office, guides the state's approach to providing high-speed, reliable internet access to the areas and people who need it the most.<br>The Link Oregon State Connectivity Phase 1 has been completed.  Migration of circuits to the Link Oregon network provides high-speed, cost-effective, fiber broadband services to Oregon-based public and non-profit organizations.  The Link Oregon Strategic Plan was adopted in April 2023.<br>This expansion of broadband capabilities continues to be a focus for Oregon. | ✓<br>Implement |

## 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 |
|---|---|---|---|
| **Zero-trust security**<br>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.<br>Unlike VPNs, which mainly authenticate users at the initial connection, zero trust network access continuously evaluates the trustworthiness of a connection, considering factors like device health, user behavior, and context. | 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.<br>EIS will continue to explore the best use of a zero-trust networking approach. | Planning |
| **Multi-cloud Access**<br>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 a 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 | Planning |

| Technology Trend | Description | CTO Perspective | EIS Adoption |
|---|---|---|---|
| | | necessary. | |
| **Network Segmentation**<br>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 |
| **Software Defined Networking (SDN) Overlay**<br>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 |
| **Cloud Access Security Broker**<br>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 |
| **Network Access Control** | 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 | |

| Technology Trend | Description | CTO Perspective | EIS Adoption |
|---|---|---|---|
| 202406-T6 | | access and non-compliant devices. | Planning |
| **Microsoft Copilots**<br>202406-T7 | There are several places where Artificial Intelligence (AI) may come into play within the Oregon Enterprise. Some of these include Microsoft Copilots. | Artificial Intelligence is a continuum of capabilities ranging from prewritten business rules to RPA to machine learning to generative AI. There is not a one size policy which covers all use cases.<br>Oregon executive leadership is providing interim guidance (link to State CIOmemo) for the Executive Branch use of AI technology while the State Government Artificial Intelligence Advisory Council completes a final recommended action plan as required by Executive Order 23-26. | Awareness |
| **Microsoft Entra ID for Customers**<br>202406-T8 | Microsoft Entra External ID platform represents the future of customer identify and access management (CIAM) for Microsoft.<br>Microsoft Entra ID for customers if Microsoft's new CIAM solution. For organizations and business that want to make their public-facing applications available to consumers, Microsoft Entra ID makes it easy to add CIAM features like self-service registration, personalized sign-in experiences, and customer account management. | Integral component of Customer Identity and Access Management (CIAM). Self-Service Registration can be available for agency public-facing applications.<br>Other features include personalized sign-in experience and customer account management. | Awareness |

| Technology Trend | Description | CTO Perspective | EIS Adoption |
|---|---|---|---|
| | https://learn.microsoft.com/en-us/entra/external-id/customers/ | | |

## 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**

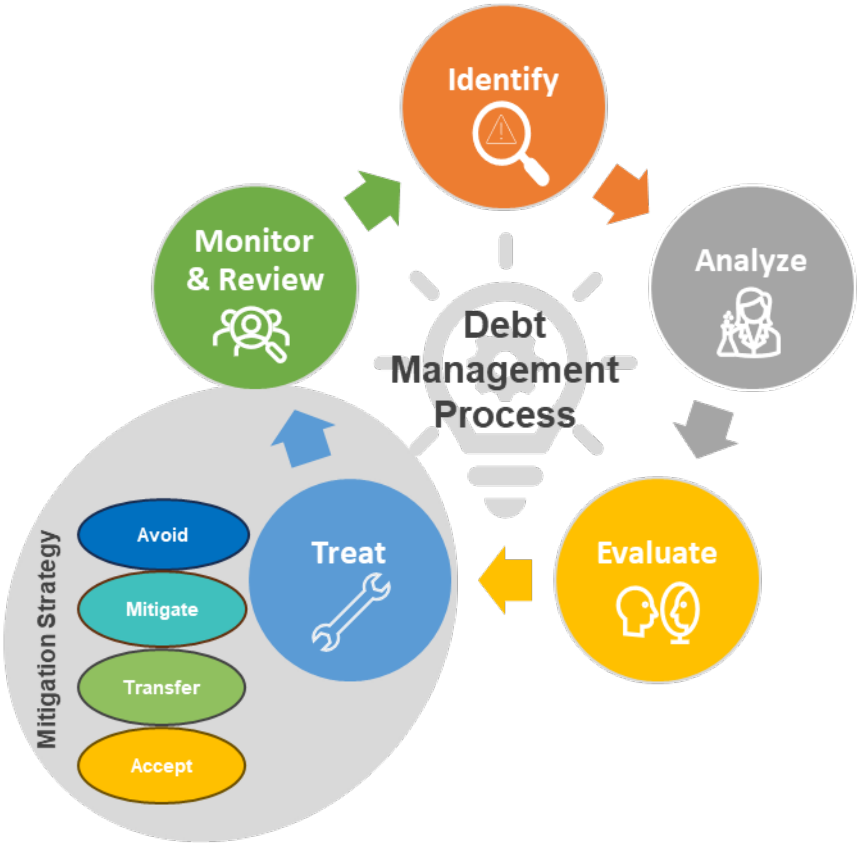


Figure 5 (Debt Management Process Steps) provides a description of the debt management process steps.

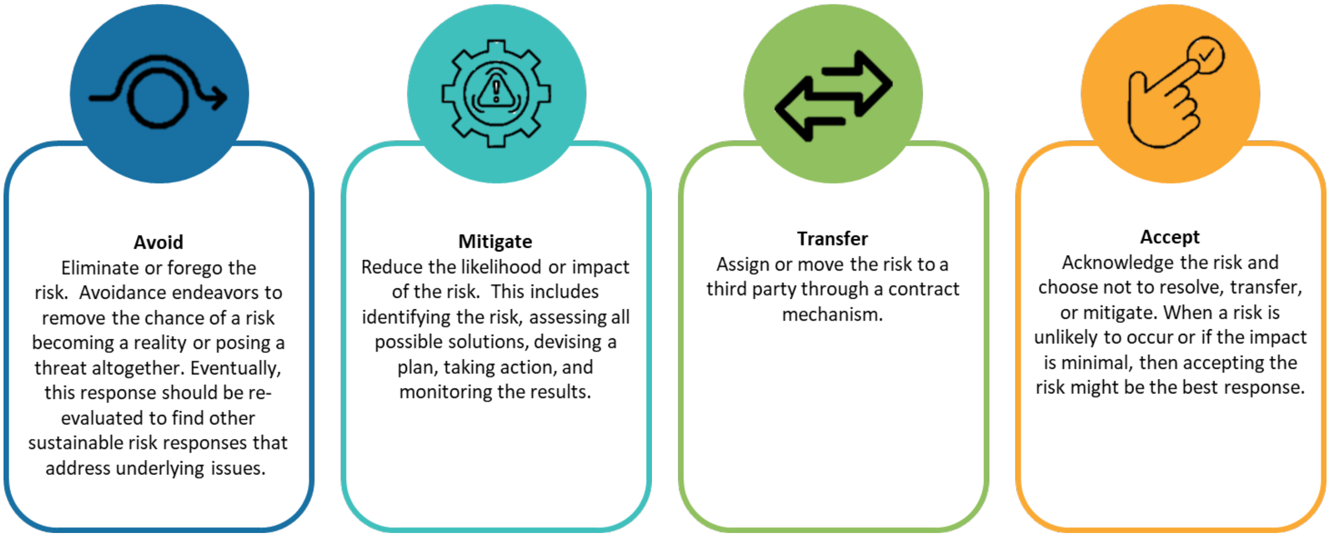
**Figure 5: Debt Management Process Steps**

| 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 |
|---|---|---|---|---|
| **Network Infrastructure** | Technical | Aging infrastructure, resiliency, etc. | | Enterprise Information Services contracted for a Network and Security |

| Debt Area | Debt Type | Description | Approach | Mitigation Strategy |
|---|---|---|---|---|
| 202406-D1 | | | Mitigate | Modernization Plan (TITAN) 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 Modernization**<br>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 | In support of the 2023-2026 EIS Strategic Framework Objective, "Mature Legacy System Modernization Strategies", S&D is:<br>• Working closely with the Assistant State Chief Information Officers (ASCIOs) to align agency modernization projects at the enterprise level.<br>• Partnering with Project Portfolio Performance (P3) to ensure new projects minimize technical debt into the environment.<br>• Evaluating application modernization services approaches including the migration from mainframe and on-premise servers into the cloud. |
| **Move Medicaid** | Technical | Support Medicaid vendor re-platform and relocation | | Continue to support Data Center Services operations of current solution while |

| Debt Area | Debt Type | Description | Approach | Mitigation Strategy |
|---|---|---|---|---|
| **System to Cloud**<br>202406-D3 |  | efforts to move primary MMIS module from the State Data Center to the cloud | Transfer | the MMIS vendor re-platforms the HP-UX servers to Linux and migrates the solution to the cloud.  Assist and monitor the transition to the new platform. |
| **Organizational Change Management**<br>202406-D4 | Organizational | Recognizing the need for responsive leadership, clear purpose and priorities, quality communication, support for change and coordination in delivery | Mitigate | Transitioning to an "as a service" delivery mode requires a fundamental shift both with contracting and business operations.<br>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. |
| **Governance**<br>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 | 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.<br>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

Enterprise Information Services and the agencies in the Executive Branch have been very busy over the past two years establishing their modernization goals.  That level of effort and energy will not change in the foreseeable future.  There has been real progress made on several fronts.

- The Microsoft 365 project standardized Identity and Access Management and streamlined the security provisioning activities across Executive Branch agencies. Additional M365 products and features will be introduced in the coming months.

- Security monitoring and reporting capabilities have been strengthened.

- Planning and guidance publications have created a common message and direction for our agencies to support their modernization activities.

Our Vision remains the same.  Ensuring accessible, reliable and secure state technology systems to equitably serve Oregonians.  As our focus begins to transition from “project” to “process”, we are establishing the appropriate governance and process rigor to assist the agencies in their modernization journey.  They expect our best.  We will deliver.

There is much to do.  Technology transition requires Organizational Change Management and preparation across the Enterprise.  Our teams are working hard to guide that evolution in a thoughtful way as we survey and plan to incorporate emerging trends and technology.  Legacy system modernization, open data, cloud, and shared services remain at the forefront of our effort while we also seek to increase our statewide digital delivery.

While S&D may be the “tip of the spear” in establishing the environment and technical strategy for the state, the day-to-daysupport to Oregonians comes from the agencies.  It is only through their efforts and dedication that any real change happens.  We are here to partner with them in their efforts to equitably meet the needs of the Oregon public.