HECC IT Strategic Plan Progress Report

Table of Contents

I. Executive Summary

This progress report provides an overview of the implementation and advancement of the IT strategic plan for the period of July 1st, 2024 through May 30, 2025. The plan aligns with the agency's overall mission and business objectives, focuses on strengthening agency digital capabilities, and enhances the operational efficiency and driving innovation.

Significant progress has been made across all strategic pillars. Key achievements include release 1 of the modernization or LEARN system, successful migration of many cloud-based services, and advancement in cybersecurity readiness. Digital transformation initiatives have accelerated, with the rollout of new data analytics platforms, and process automation tools improving service delivery and decision making.

Governance structures have ensured transparency, alignment with enterprise priorities, and effective risk management. Challenges encountered, such as resource constraints and SI vendor performance are being addressed through adaptive planning and continues improvement mechanism.

Looking forward, the revised strategic plan will continue to build on last year to expand the digital integration, optimizing our security posture, and ensuring technology investments deliver measurable value. The IT division remains committed to innovation, resilience and enabling organization success through strategic technology leadership.

II.   Strategic Objectives

Strategic Objectives	Progress made towards each objective
Achieve IT Operational Excellence	Although much progress has been made towards achieving this strategic objective such as establishing a platform architecture and development environment, more work remains to complete the agency modernization effort. The SI vendor has completed the ETPL in-scope functionality. The deferred ETPL functionality and all scope for PCSVets and FAMIS is being re-evaluated and the agency intends to publish an RFP for a new vendor to complete the remaining scopes.
Effective Data and Analytics	HECC has established data and information governance and an accountability structure. The agency believes this work will improve data accessibility, data integrity, and enhance comprehensive reporting capabilities. Towards that goal, HECC has done extensive work in collaboration with InfoTech Consulting Services and has been executing to strengthen the agency data and information governance.
Improve Security Posture	The agency has improved its overall security posture from the previous year based on the EIS/CSS security audit findings and many other security initiatives that it has deployed. The agency CIS control set implementation score increased from 40% to 52.5% in the last year, however, more work remains to meet the expected enterprise goal of 70%. All agency employees successfully completed the annual IT DAS - EIS - 2024 Information Security Training: Foundations. The agency also hybrid-joined its devices to improve cyber security detection and prevention. Also, our phishing failure rate has improved from 32% to less than 5% as of today.

III.   Metrics and Targets

IT Goals	Business Facing Objectives	Target Metrics	Outcome
Achieve IT Operational Excellence	• Customer Satisfaction • Project success rates • Application reliability and stability	• Establish baseline and Improve response time by 5% YoY • Establish baseline and Reduce support calls by 5% YoY	• Baseline established in July 2024 at 80%
Effective Data and Analytics	• Alignment of data collection to business needs • Database consolidation • Single source of truth	• Consolidate existing databases to Azure within 12 months • Data governance process set up within 12 months	• Both initiatives are Completed
Improve Agency Security Posture	• Cyber Security Improvement • Cyber Security Awareness	• Increase the agency CIS control implementation goal from 40% to 80% • 100% HECC employees complete the cybersecurity awareness training and increase of detection rate	• See Appendix I. Link to the CSS assessment report • 99% of employee completed*

- - * 1 incomplete was for an employee out on protected leave

IV. Initiatives

1. Business-Supporting IT Initiatives

a. *Establish Platform Architecture and Development Environment:*

HECC contracted with an SI vendor to establish a solution architecture and development environment as part of the modernization project or LEARN system. Most of the task is complete. The SI vendor and agency are now working on an O&M transition plan that includes documentation, staff training and knowledge transfer among other activities. Agency is assessing on how best to leverage the platform to transition other legacy system to this environment, see below 2.d.

b. *Support the replacement of ETPL, FAMIS, and PCS Vets*

The SI vendor has completed the ETPL in-scope functionality successfully, and the system has gone live first week of May without any major issues. However, the SI vendor has pulled out of the LEARN project. The deferred ETPL functionality and PCS Vets and FAMIS replacement scope are now being re-evaluated. The agency plans to publish an RFP for a new vendor to complete the project once the contract separation with the SI vendor is finalized.

c. *Improve Data Architecture and Governance*

HECC has established data and information governance and accountability structure. The agency believes this work will improve data accessibility, data integrity, and enhance comprehensive reporting capabilities. Towards that goal, HECC has done extensive work in collaboration with InfoTech Consulting Services and has been executing to strengthen the agency data and information governance.

2. IT Excellence Initiative

a. *Strengthen IT Strategy and Governance*

HECC contracted InfoTech Research Group to assist developing its IT Strategic Plan and revamp its governance structure. After completing the IT Strategic Plan, the agency initiated the development of an updated IT governance model to clarify decision-making processes and accountability. We engaged key stakeholders across departments to ensure alignment and buy-in and begun drafting key polices to support improved oversight, risk management, and performance tracking. Next steps include adopting the revised strategic plan and presenting the annual progress report.

b. *Grow DevOps Capability, Skillsets, and Resource Plan*

The agency initiated a phased DevOps implementation roadmap which started with CI/CD pipeline enhancements and environment automation. Working with Microsoft, we launched targeted training sessions to strengthen internal skillsets in cloud-native tools, infrastructure as code, and agile practices. Migrated the development environment to Azure and conducted a capability assessment to identify skill gaps and inform our upskilling and recruitment strategy. Refined our resource plan to ensure we have the right mix for internal talent and external support to meet business needs.

c. *Improve the Agency Security Posture*

The agency worked in aligning our cybersecurity effort with the State of Oregon security standards and enhanced incident response capabilities through tabletop exercises, and playbook updates. Using State security apparatus, we established a continuous vulnerability assessment and patching cycle, improving remediation timelines and all agency devices were hybrid-joined to the State. The agency participated in the mandatory cybersecurity training across the agency and increased our phishing simulation resilience where the failure rate reduced from 32% to less than 5% today. In addition, the agency has improved the EIS/CSS security assessment results to 52.5%, see appendix I for reference.

d. *Migrate Other Legacy Systems to the Platform*

Not much progress is made on this regard since the key priority in the last year has been the agency Modernization Project. However, there has been many bug fixes, updates, and enhancement work done over the past year.

e. *Implement Unified Data Analytics Solution*

Successfully implemented and deployed PowerBi as a centralized analytics platform that integrates data from key operational systems, enabling cross-functional insights. Rolled out self -service dashboards and reporting tools to empower business units with real-time insights and reduce reliance on manual reporting. The agency also established a data governance committee and model to ensure that data quality, consistency, and compliance aligns with the State of Oregon standards as well as federal rules and laws.

f. *Establish Project Portfolio Management Structure*

We have not made much progress this year due to lack of budget and to the modernization project being higher priority. However, staff continue to acquire project management skill working on the modernization project. Moreover, the agency plans to hire a project manager when the agency proposed budget is approved.

3. IT Initiative Supporting Innovation

a. *Advance HECC's Mission Through Artificial Intelligence*

This past year staff spent building an AI strategy for the agency. We have worked with InfoTech Advisory Group on how best to align with the State of Oregon AI recommended Action Plan as we implement and deploy our Ai strategy.

V.   Resource Allocation

HECC is a small organization and all the IT personnel in one way or another support in achieving its IT strategic plan. The agency IT budget, technology and resources are fully dedicated in support of the agency strategic plan goals.

Information Technology Budget Overview	
Category	**Budget**
2. Personal Services	5,312,868
General Fund	4,152,798
Other Funds	643,282
Federal Funds	516,788
3. Services & Supplies	798,601
General Fund	537,863
Other Funds	95,000
Federal Funds	165,738
4. Capital Outlay	8,650,157
5. Special Payments	-
Total	**14,761,626**

VI.   Risks and Mitigation Strategies

The following are the top three risks the agency considers may impact the plan objectives and strategies in place to mitigate them:

Risk	Description	Mitigation Plan
Resource Constraints	Limited budget, staffing, or legislative priority changes	Conduct regular resource planning; prioritize critical initiatives; leverage cross-training, upskilling, and strategic partnerships; advocate, lobby for sufficient funding.
Vendor Dependence	Vendor performance or continuity issues affect outcomes.	Diversify vendors where possible; negotiate strong contract and agreements; develop exit and contingency plans for critical services.
Data quality and integration issues	Inconsistent or siloed data undermines insights.	Establish a robust data governance program; use data profiling tools; enforce standards for data stewardship and integration

VII.   Next Steps and Conclusion

This being the first year to provide progress report, most of our performance metrics are sparse. In the upcoming year, we intend to institutionalize governance and metrics where we establish a performance dashboard to monitor progress across all the strategic initiatives, and to regularly report metrics to our Information Technology governance committee to ensure accountability and alignment.

The agency has been able to implement a Dynamics 365 platform and modernize one out of three program areas. However, the System Integrator Vendor informed the agency that the project cost would be three times more than they had originally anticipated. The agency is researching at other options for the modernization project next steps accordingly.

Appendix I:

HECC Overall CAS Score

52.5%

Enterprise Goal
70%

Average Across NIST CSF Security Functions: HECC

Function	Wt Ave Across Function
GOVERN	
IDENTIFY	41%
PROTECT	48%
DETECT	84%
RESPOND	
RECOVER	
UNMAPPED	63%

Enterprise Goal: 70%

CIS Control #1 — Asset Inventory: 83%

CIS Control #2 — Software Inventory: 70%

CIS Control #3 — Data Protection: 6%

CIS Control #4 — Secure Configuration: 38%

CIS Control #5 — Account Management: 72%

CIS Control #6 — Access Control: 31%

CIS Control #7 — Vulnerability Management: 92%

CIS Control #8 — Audit Log Management: 24%

CIS Control #9 — Email & Browser Protection: 100%

CIS Control #10 — Malware Defense: 100%

CIS Control #11 — Data Recovery: 0%

CIS Control #13 — Network Monitoring and Defense: 21%

CIS Control #14 — Security Awareness & Training: 99%

CIS Control #15 — Svc. Provider Management: 0%

CIS Control #17 — Incident Response: 0%

CIS Control #18 — Penetration Testing: 0%

Legend:
- 70% or Above - Meets Expectations
- 51% - 69% - Needs Improvement
- 26% - 50% - Poor
- 1% - 25% - Extremely Poor
- Not Implemented