IT Strategic Plan Progress Report

June 1, 2025

State of Oregon
DEQ Department of Environmental Quality

This document was prepared by
Oregon Department of Environmental Quality
Information Technology
700 NE Multnomah Street, Suite 600
Portland Oregon, 97232
Contact: Contact
Phone: 503-555-5555
www.oregon.gov/deq

State of Oregon
DEQ Department of Environmental Quality

Executive summary

The purpose of Oregon Department of Environmental Quality’s annual IT Strategic Plan Progress Report is to provide constituents and other interested parties with valuable insights into performance.

At a high level, DEQ made significant progress against the previously determined IT strategic objective “Security of information, processing infrastructure and applications, and privacy”, and some improvements on other objectives, however, there are opportunities for improvement across all five IT strategic objectives.

DEQ
State of Oregon
Department of Environmental Quality

Some of the most significant progress against the IT strategic objectives happened quickly in response to the unprecedented cyber incident DEQ experienced. DEQ has been taking several steps to mitigate the risk of cyber vulnerabilities. This includes leveraging Oregon state’s Cyber Security Services expertise and migrating servers to the Oregon State Data Center; utilizing next-generation protection against malware, phishing, and ransomware; updating cyber security processes and restricting administrative access for their work and providing additional training for DEQ regarding cyber security best practices and associated state policies.

Table of contents

Strategic Objectives

DEQ's IT alignment objectives and current performance against them are below.

Table 1. Summary of DEQ IT's performance against alignment objectives.

IT Alignment Objectives	Performance Against IT Alignment Objective
Delivery of IT services in line with business requirements	IT Service Desk: • 85% service level agreement success rate. • Average 5/5 stars for customer satisfaction. Your DEQ Online Helpdesk: • 99% service level agreement success rate. • Average 4.8/5 stars for customer satisfaction.
Managed IT-related risk	Worked with the DEQ's Chief Auditor to create the Information Services Risk Assessment and identified risks in the following categories: cybersecurity, governance, operational, user and access.
IT compliance and support for business compliance with external laws and regulations	Need to identify the external laws and regulations to be evaluated and the criteria for compliance for each law and regulation to enable recording of progress.
Security of information, processing infrastructure and applications, and privacy	• Leveraged Oregon state's Cyber Security Services expertise and migrating servers to the Oregon State Data Center. • Utilized next-generation protection against malware, phishing, and ransomware Updated cyber security processes and restricting administrative access. • Provided additional training for DEQ regarding cyber security best practices and associated state policies.
Realized benefits from IT-enabled investments and services portfolio	• Utilized the DAITM (DEQ Agency-Wide Information Technology Management) Committee which provides IT governance framework. • Established updated DAITM scoring matrix to verify that DEQ prioritizes, selects, and monitors IT investments to ensure optimal allocation of resources and that they are in alignment with the DEQ business.

Metrics and Targets

The following summarizes the metrics and targets for each of IT's strategic objectives.

IT Strategic Objective 1: Delivery of IT services in line with business requirements.

a. Percent of users satisfied with the quality of IT service delivery increases over time.
b. The percent of met service level agreements increases over time.

IT Strategic Objective 2: Manage IT-related risk.

- Risks identified during regular IT risk assessments over time.

IT Strategic Objective 3: Ensure IT compliance with external laws and regulations.

- Have zero un-remediated IT-related noncompliance issues reported.

IT Strategic Objective 4: Ensuring security of information, processing infrastructure and applications.

- Achieve a 90% resolution rate for all identified vulnerabilities within 30 days of detection. Speed in addressing vulnerabilities is crucial to maintaining the integrity of our software. This metric will ensure that our team prioritizes and acts swiftly upon the findings of our security assessments.
- The number of confidentiality, integrity, or availability incidents causing financial loss, business disruption is zero.
- Achieve equivalent implementation percentages of at least 40% across the following four categories by the end of 2024: Procedures Complete, CIS Controls 1-6 efficacy, CIS Controls 1-6 automated, and CIS Controls 1-6 reported. DEQ is targeting a compliance level of 40% because the agency values security and intends to make it difficult for attackers to compromise systems and gain unauthorized access to sensitive data. This contributes to the protection of the agency's information assets and ensures the continuity of essential services.
- Decrease average security incident response time by 5% over the next fiscal year. A quicker response time is vital in limiting potential damage during a security incident. The team will be equipped with tools and protocols to act swiftly during such events.

IT Strategic Objective 5: IT-enabled investments and services portfolio.

- 100% of IT-enabled investments for which claimed benefits in the business case are met.
- Complete the transition into Your DEQ Online, a cloud platform, of 100% of the agency's in-scope permitting, licensing, and certification programs in 2024. This will reduce maintenance and infrastructure costs, increase scalability, and improve the agency's efficiency and quality of service to all of Oregon's inhabitants.

- Achieve a consistent 80% or above Key Performance Indicator, or KPI, target attainment rate across all software development projects. By aiming for a high KPI attainment rate, we set a standard of excellence for our team. This target will motivate the software development team to consistently deliver high-quality outputs that realize the anticipated benefits.
- Achieve a 20% increase in project lessons learned for projects that go through DEQ's IT project governance framework. By actively applying insights from past projects, we aim to continually refine our processes and methodologies. This metric ensures that the team integrates lessons learned into their workflow, leading to more successful and efficient project executions.
- Achieve a 90% alignment rate between new IT initiatives and the agency's strategic objectives within a year. By ensuring that the majority of new projects directly support our goals, we optimize resource utilization. This metric serves as a benchmark, driving the team to always align their efforts with the agency's mission.

Initiatives

These are the initiatives under each of DEQ IT's strategic objectives.

1. **IT Strategic Objective 1: Delivery of IT services in line with business requirements:**
   a. Roll-out a unified requirement documentation system.
   b. Implementing a robust IT Service Management framework to effectively deliver IT services and manage service level agreements.
   c. Create a culture of continuous improvement by improving the satisfaction of the quality of IT service percent over time.
2. **IT Strategic Objective 2: Manage IT-related risk:**
   a. Partner with Cyber Security Services to continually improve its policies, procedures, and controls to mitigate IT risks, such as data breaches, system outages, and cybersecurity threats.
   b. Engage in routine risk assessments and audits, in collaboration with Cyber Security Services and the Secretary of State, to identify, assess, and prioritize potential risks and vulnerabilities, enhancing the agency's security and compliance posture.
   c. Create a culture of continuous improvement by the risk assessment scores improving over time.
3. **IT Strategic Objective 3: Ensure IT compliance with external laws and regulations:**
   a. Update the IT initiative process to include an evaluation to confirm compliance with external laws and regulations.
   b. Create a culture of continuous improvement by recording the number of IT related noncompliance issues reported or causing public embarrassment and taking action to prevent the issue in the future.
4. **IT Strategic Objective 4: Ensuring security of information, processing infrastructure and applications, and privacy:**
   a. Remediate prioritized security gaps identified within the 2023 CSS assessment.

b. Work closely with Cyber Security Services to implement a robust information security program. A multi-layered approach to security is crucial, encompassing network, application, and endpoint security measures.
c. Performing regular vulnerability assessments, penetration tests, and security audits will be conducted to identify and address potential weaknesses.
d. Create and maintain a robust incident response plan that helps to quickly detect, respond to, and recover from security incidents.
e. Maintain privacy best practices, such as data minimization and encryption to ensure the privacy of personal and sensitive information.

5. **IT Strategic Objective 5: Realized benefits from IT-enabled investments and services portfolio:**
    a. DAITM committee will work continually to improve the agency's IT governance framework.
    b. Ensure IT investments align with the agency's objectives and deliver value. The portfolio management process (DAITM scoring matrix) will guide the agency as it effectively prioritizes, selects, and monitors IT investments to ensure optimal allocation of resources.
    c. Establish and track KPIs will enable DEQ to measure the performance and benefits realization of IT investments and services.
    d. Conducting regular post-implementation reviews and lessons learned sessions will help identify opportunities for improvement and optimize the return on IT investments.

Resource Allocation

DEQ's Information Services is comprised of 40 individuals which includes a Chief Information Officer, Chief Technology Officer, Manager of Helpdesk, Manager of Your DEQ Online enterprise system, and a Software and Development Manager.

DEQ has requested two new positions in the Information Services division:

ISS4 Your DEQ Online System Helpdesk: This position would report the Your DEQ Online Manager within the Information Services organization. This position will provide support for the internal and external customers of the Your DEQ Online system. The Your DEQ Online system is the permitting, certification, and licensing platform that is used by the regulated community to apply for permits, certifications, and licenses and pay for the business services DEQ provides. DEQ staff also use the Your DEQ Online system to manage their work. The public also use the Your DEQ Online system to access general public records requests.

ISS7 Enterprise System Administrator: This position would report to the IT Operations Manager within the Information Services organization. This position will coordinate and provide strategic direction, enterprise-wide planning, research, design, development, implementation, and operational support of agency-wide IT systems and services. This position will also work closely with The State of Oregon's Cyber Security Services, which is responsible for defining enterprise security architecture and policy and for coordinating security incident response. In partnership with CSS, this position will serve as an on-site counterpart at DEQ to implement State security standards and best practices, consult on agency technology initiatives, conduct security risk identification and remediation, and assist in security incident response activities. The creation of this position will reduce the advanced infrastructure management and security implementation workload from existing staff who are over-extended, ensuring the agency can keep pace with the rapidly changing technology environment.

Risks and Mitigation Strategies

DEQ has actively worked on the Continuity of Operations Plan which is critical for ensuring that any organization can continue its essential functions during and after a significant disruption. A sub-component of the plan is the Information Technology Disaster Recovery Plan, or ITDR. An ITDR restores mission critical systems in the most efficient way possible so that the cost in dollars and time due to disruptions can be minimized.

During the creation of the DEQ ITDR, systems were identified and prioritized. The resulting ITDR includes a list of mission critical systems. As mentioned, DEQ is currently in the recovery phase of a cyber incident and the ITDR has been instrumental in ensuring that resources are utilized in the most efficient way possible.

DEQ has been taking several steps to mitigate the risk of cyber vulnerabilities. This includes leveraging Oregon state’s Cyber Security Services expertise and migrating servers to the Oregon State Data Center; utilizing next-generation protection against malware, phishing, and ransomware; updating cyber security processes and restricting administrative access to only those who need it for their work and providing additional training for DEQ regarding cyber security best practices and associated state policies.

Next Steps

DEQ’s next steps are to evaluate the previously completed Information Services risk assessment and identify if updates need to be made due to the most recent cyber security hardening activities. Based on the findings, updates to the IT Strategic Objectives may be made. The metrics for each IT Strategic Objective will be reviewed for relevance and updated if more appropriate ways to measure are determined.

In addition, DEQ plans to perform a cyber incident lesson learned process after all business systems are restored. DEQ plans to leverage the Cyber Security Services After Action report when available. DEQ plans to learn as much as possible from the cyber incident experience. This process will help DEQ to identify what worked well and what could be improved. This is an excellent opportunity for improvement, growth, and overall maturity of the organization.

Conclusion

In conclusion, DEQ made significant progress against the previously determined IT strategic objective “Security of information, processing infrastructure and applications, and privacy,” and some improvements on other objectives, however, there are opportunities for improvement across all five IT strategic objectives.

Some of the most significant progress against the IT strategic objectives happened very quickly in response to the unfortunate cyber incident DEQ experienced. DEQ has been taking several steps to mitigate the risk of cyber vulnerabilities. This includes leveraging Oregon state’s Cyber Security Services expertise and migrating servers to the Oregon State Data Center; utilizing next-generation protection against malware, phishing, and ransomware; updating cyber security processes and restricting administrative access to only those who need it for their work and providing additional training for DEQ regarding cyber security best practices and associated state policies.