IT Annual Report

2025

CONTENTS

Executive Summary

This year marks a pivotal point in the evolution of technology at the Oregon Department of Emergency Management. For the first time, OEM has a dedicated Chief Information Officer guiding a comprehensive IT vision that spans infrastructure, logistics, facilities, and fleet management. We've laid foundational cornerstones through the development of both our Agency Strategic Plan and our first IT Strategic Plan, ensuring IT is directly aligned with OEM's mission and operations.

Perhaps most notably, OEM has successfully executed its first independently led IT project, demonstrating growing maturity and capability in managing complex technology initiatives. This independence reflects a broader cultural shift toward accountability, innovation, and streamlined operations.

Throughout the year, we've focused on realigning priorities, sunsetting ineffective tools, and adopting new systems that better serve our stakeholders. We've made progress in standardizing workstations, integrating IT with financial processes, and supporting staff through transitions and new hires. While change has been constant, it has also been purposeful, building a future-ready foundation for service, safety, and resilience.

As we look ahead, we are energized by the opportunities before us and committed to delivering high-impact, mission-aligned technology services that empower our agency and the communities we serve.

Strategic Objectives

The following strategic objectives, as outlined in OEM's IT Strategic Plan, provide the foundation for technology decisions, investment planning, and service delivery across the agency:

- Advance mission delivery through digital modernization: Implement flexible and scalable technologies that enhance OEM's ability to respond quickly and effectively to emergencies.
- Enable a secure, resilient, and adaptive infrastructure: Build IT systems and networks that can sustain evolving operational demands while withstanding cyber and physical threats.
- Promote information as a strategic asset: Improve the accessibility, quality, and governance of data to support informed decision-making and performance measurement.
- Deliver excellent IT services and user experience: Strengthen service delivery through process improvements, automation, and enhanced support tools that meet customer needs.
- Strengthen IT governance and operational transparency: Formalize oversight structures and communication pathways to align IT initiatives with enterprise strategy and ensure accountability.

- Develop a skilled and agile IT workforce: Invest in training, professional development, and collaborative practices that empower staff to meet current and future technological demands.

Metrics and Targets

OEM will use a strategic metrics framework to evaluate progress across its six IT Strategic Objectives. These metrics provide transparency, inform decisions, and guide future planning.

1. Digital Modernization

- % of legacy systems replaced or retired
- % of systems migrated to modern, cloud-based platforms
- Time to deploy business solutions (from request to implementation)

2. Secure and Resilient Infrastructure

- % of critical systems with documented business continuity plans
- Number of successful disaster recovery tests per year
- % of systems achieving target uptime (99.9%)

3. Information as a Strategic Asset

- % of systems with applied data classification
- Number of active datasets published to internal or external dashboards
- % of compliance with data governance standards

4. Excellent IT Services and User Experience

- Average helpdesk ticket resolution time
- User satisfaction score (based on annual survey)
- % of service catalog items automated or self-service enabled

5. Governance and Operational Transparency

- % of projects reviewed and tracked by the IT Governance Committee
- % of strategic roadmap milestones achieved on schedule
- % of initiatives linked to agency strategic goals

6. Skilled and Agile Workforce

- % of IT staff completing annual professional development
- % of roles with defined training plans and skill assessments
- Participation in cross-functional project teams

Metrics will be reviewed quarterly with updates provided to executive leadership as part of the IT Governance reporting cycle.

IT Initiatives

The Oregon Department of Emergency Management (OEM) is actively executing a comprehensive portfolio of IT projects to modernize operations, support emergency preparedness, and enhance agency-wide efficiency. These initiatives are aligned with OEM's IT Strategy Plan and are essential to building a resilient, mission-ready technology environment.

IT Governance Framework – Establishes a structured decision-making body for prioritizing IT investments, ensuring strategic alignment, and monitoring execution. The Governance Committee, launching in June, will oversee project approvals, resource allocations, and performance metrics.

Grants Management Modernization – Replaces manual tracking with a fully automated, end-to-end digital platform that supports grant application, monitoring, and reporting. This system improves compliance, reduces processing times, and enhances visibility across the grant lifecycle.

Task Management System – A Microsoft 365-based solution developed in-house to centralize tracking of agency actions, assignments, and deliverables. The tool promotes accountability, transparency, and agility through real-time status updates and role-based workflows.

Crisis Management System (OpsCenter) Replacement – A phased effort to replace OEM's 20-year-old emergency response coordination platform. Initial work includes requirements gathering, stakeholder engagement, and risk mitigation planning. The system will ultimately improve incident response, resource tracking, and interagency coordination.

Integrated Watch Center Enhancements (OERS Transition) – Prepares OEM to assume operational control of the Oregon Emergency Response System from OSP. Efforts include facility upgrades, hardware modernization, and new dispatch and alerting tools to support 24/7 situational awareness.

Data Center Services Migration – In response to end-of-life hardware, OEM is migrating critical services to cloud-hosted or co-located environments. This shift ensures service continuity, improves security, and reduces maintenance costs.

Learning Management System (LMS) – Collaboratively developed with OSFM, OSP, and DPSST, this platform will standardize training delivery, ensure compliance tracking, and provide a user-friendly interface for professional development across emergency management disciplines.

Next Generation 9-1-1 (NG911) – A multi-agency project to modernize emergency communications by deploying IP-based systems that support voice, text, and multimedia. The initiative enhances location accuracy and improves routing to the appropriate public safety answering point (PSAP).

Oregon Records Modernization (ORMS) – Aligns OEM's records management with statewide standards for digital documentation, retention, and access. This includes appointing a records officer and deploying policy-based tools for lifecycle governance.

M365 Governance and Standardization – Streamlines usage of Microsoft 365 tools by implementing governance policies, optimizing licenses, and reducing site sprawl. Training and adoption campaigns are underway to enhance user effectiveness.

Service Desk Modernization – The outdated helpdesk appliance has been replaced with ManageEngine's cloud-based ITSM platform. The roadmap includes asset tracking, self-service portals, and integration with project and knowledge management systems.

Procurement Tracking System – A low-code application built in Power Apps that digitizes procurement requests, automates approval workflows, and generates real-time reports to support transparency and audit readiness.

Fleet Key Kiosk System – A secure, automated solution for managing fleet vehicle access and logging usage data. The kiosk improves accountability, reduces manual errors, and integrates with OEM's asset tracking systems.

Workstation Modernization – Replaces outdated devices and standardizes OEM systems on Windows 11. This improves security, enables advanced features, and supports hybrid and remote work environments.

Business Continuity and Disaster Recovery Planning – Developing a robust BC/DR strategy aligned with OEM's Continuity of Operations Plan. This includes risk assessments, backup standards, and recovery testing protocols for critical systems.

Identity and Access Management (IAM) Enhancements – Strengthens access controls through better role definitions, automated provisioning/deprovisioning, and enhanced audit logging. This supports compliance with cybersecurity frameworks.

These initiatives reflect OEM's strategic focus on secure, adaptable, and mission-aligned technology that meets the demands of emergency response and public safety.

Resource Allocation

To support strategic IT initiatives and maintain operational stability, OEM must ensure thoughtful allocation of financial, technical, and human resources. The following areas define how resources are being aligned with agency priorities:

Budget Planning

- OEM is working toward a dedicated IT budget structure that enables proactive investment, lifecycle planning, and modernization. This includes seeking legislative support and optimizing grant utilization.

Funding Alignment

- Projects such as Crisis Management System Replacement and LMS deployment are strategically aligned with federal and state funding opportunities. Timing and execution depend heavily on coordination with grants and legislative cycles.

Staffing and Expertise

- Existing staff are cross trained to manage multiple systems and responsibilities. However, there are critical gaps in business analysis, project management, and system architecture. Temporary contractors help bridge the gap for high-priority initiatives.

Infrastructure Investment

- Resources are being allocated to upgrade aging systems, complete the Windows 11 rollout, and migrate workloads from end-of-life servers to sustainable environments.

Tooling and Platforms

- Investment continues in platforms that support self-service, automation, and scalability, especially through M365, ManageEngine, and low-code tools like Power Apps.

Governance and Accountability

- The new IT Governance Committee plays a vital role in reviewing resourcing decisions, prioritizing initiatives, and aligning technology investment with strategic goals.

Risks and Mitigation Strategies

Effective risk management is critical to the success of OEM's IT initiatives. The following key risk areas and corresponding mitigation strategies are drawn from lessons learned and planning outlined in the IT Strategic Plan:

1. Resource Constraints

Risk: Limited staffing and dependency on contractors may delay project execution.

Mitigation: Prioritize high-impact projects, use phased implementations, and advocate for dedicated project and analyst roles.

2. Budget Uncertainty

Risk: Absence of a dedicated IT budget limits proactive planning.

Mitigation: Align requests with legislative and grant cycles; develop business cases and pursue interagency collaborations.

3. Legacy System Dependencies

Risk: Older systems lack resilience and security, increasing risk of failure.

Mitigation: Accelerate migration to modern platforms and integrate failover protocols into critical systems.

4. Cybersecurity Threats

Risk: Increasing cyber threats pose a risk to data integrity and availability.

Mitigation: Enhance IAM, endpoint protection, and BC/DR planning; implement continuous monitoring and policy enforcement.

5. Change Management

Risk: User resistance to new systems may hinder adoption.

Mitigation: Invest in training, stakeholder engagement, and phased rollouts to build user confidence.

6. Governance Gaps

Risk: Without active governance, initiatives may drift from strategic priorities.

Mitigation: Ensure regular governance meetings, enforce project reporting, and maintain transparency.

These risks and mitigations will be reviewed quarterly through the IT Governance Committee and updated as part of the agency's ongoing risk management process.

Next Steps

As OEM completes the current phase of strategic planning and execution, the following next steps will guide ongoing progress:

- Finalize and operationalize governance processes through regular committee meetings and project oversight reviews.
- Track progress on key IT roadmap deliverables and provide quarterly updates to executive leadership.
- Secure sustained funding and staffing resources through budget proposals, grants, and legislative engagement.
- Develop training and onboarding materials to support broader adoption of new systems.
- Establish dashboards and reporting mechanisms to monitor strategic metrics and roadmap alignment.
- Conduct stakeholder engagement to refine future modernization priorities based on performance and evolving needs.
- These next steps will ensure momentum is maintained and that IT continues to deliver meaningful, mission-aligned value to OEM and its stakeholders.

Conclusion

OEM’s technology environment has entered a period of intentional growth and strategic alignment. The progress made over the past year—from launching new platforms and modernizing legacy systems to establishing governance and building staff capacity—lays the foundation for a more agile, secure, and mission-focused IT future.

As the agency continues to navigate increasing demands and limited resources, our commitment to operational excellence, innovation, and stakeholder engagement remains strong. Continued focus on execution, accountability, and adaptive planning will be essential to realizing the goals outlined in this report.

This report reflects not only past accomplishments but also a forward-looking vision to ensure IT at OEM is positioned to deliver meaningful and measurable impact across Oregon’s emergency management landscape.

OREGON DEPARTMENT OF

OEM

EMERGENCY MANAGEMENT