OREGON PERS

PUBLIC EMPLOYEES RETIREMENT SYSTEM

IT Strategic Plan Progress Report

October 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This quarter, the Oregon Public Employees Retirement System (PERS) Information Services Division (ISD) advanced strategic execution by strengthening performance across key measures. A heightened focus on business value continues to guide how technology investments are planned and delivered. Continued advancements in the Modernization Program—including completion of the Pension Administration System solution decision—has propelled the agency into a pivotal phase of execution. Strategic alignment, organizational readiness, and disciplined delivery will be critical to success moving forward.

PERS' mission to "*Administer public employee benefit trusts to pay the right person the right benefit at the right time.*" is grounded in accurate data, timely contributions, and precise benefit processing (OP1–OP6)[1]. Achieving this at scale requires secure, reliable, and purpose-built systems, which ISD delivers through the core supporting process of Providing Information Technology (SP3). With clearly defined performance measures and aligned sub-supporting processes, ISD enables a direct connection between mission, values, and operational execution.

This report examines how this quarter's progress aligns with the four core values at the heart of the agency's strategy—and confirms that all four remain on track, with performance indicators showing green status across the board.

---

[1] (Operational Processes 1-6—Refer to the PERS' Fundamentals Map, a key artifact in the PERS Outcome Based Management System, the PERS IT Strategic Plan, and the PERS Strategic Plan)

FOUR CORE VALUE AREAS

Core Values in Context

- **Service-focus**: Customer-centricity is at the heart of ISD's service delivery strategy—driving operational excellence and trust with members and internal users alike.

- **Accountability & Integrity**: ISD ensures that all systems are designed for transparency and traceability, reinforcing public trust through secure, auditable, and well-governed operations.

- **Professional, Accurate, Judicious**: Precision, compliance, and thoughtful execution define ISD's approach to technology—ensuring that benefit determinations and workflows are consistently accurate, fair, and policy-aligned.

- **Vigilant**: Protecting member and agency data is a top leadership priority—ISD applies layered cybersecurity practices, proactive monitoring, and rigorous controls to uphold confidentiality, trust, and legal compliance.

Service-focus

Strategic Objective: Deliver responsive, user-centered IT services that enhance internal efficiency and external member satisfaction.

Key Results (OKRs)[2]

- Increase Help Desk Service Level Agreement adherence to **≥95%** of tickets resolved within target timeframes.

- Achieve **≥90%** self-service portal uptime and issue resolution satisfaction.

- Support **100%** of agency-wide omni-channel communication milestones for member engagement.

Measures

- Help Desk Responsiveness (tickets resolved on time)

- System Uptime (% of production hours)

- Self-service portal usage and satisfaction surveys

- Member CSAT (Customer Satisfaction) from omni-channel service touchpoints

---

[2] Objectives and Key Results

Highlighted Measures:

Help Desk Responsiveness
Help Desk Responsiveness is a key performance indicator which assesses our adherence to established service level agreements (SLAs) by measuring the percentage of incident and service request tickets closed within the defined timeframes during the reporting quarter. This metric directly reflects our commitment to timely issue resolution and service delivery.

- Help Desk SLA adherence: 92%
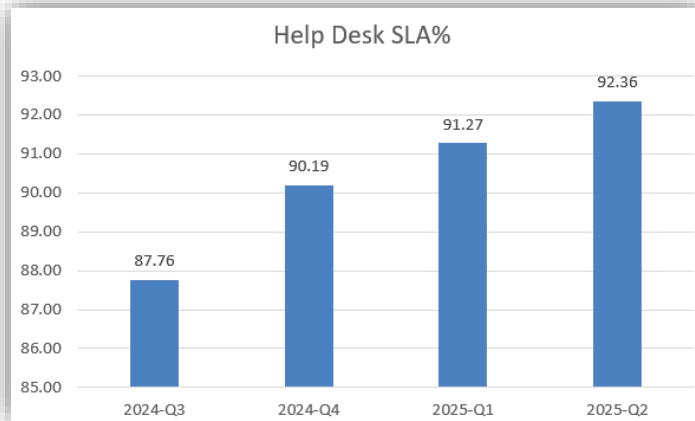
System Availability
System availability is a critical indicator of IT effectiveness, encompassing both uptime and service continuity. The System Uptime percentage measures the availability of PERS IT systems during established production hours, with higher uptime supporting operational efficiency, user productivity, and overall service delivery.
In tandem, the Service Interruption metric tracks the average number of days per month with disruptions to IT services. Minimizing these interruptions is essential, as reliable system access is foundational to processing retirements and maintaining core business operations.

- System Uptime: 99.1%
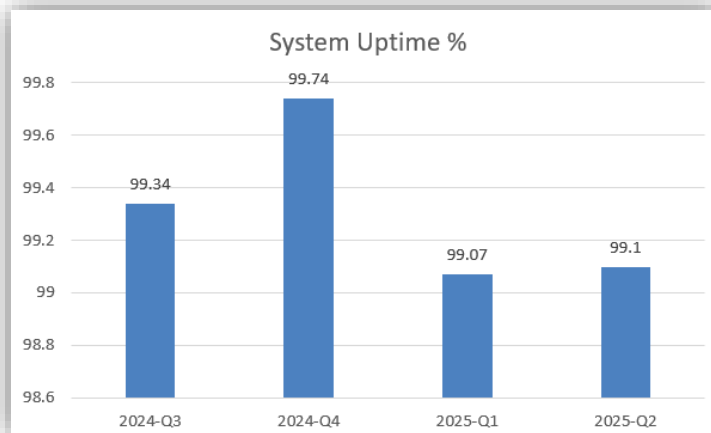
Accountability & Integrity

Strategic Objective: Ensure all IT-supported business operations are traceable, secure, and compliant with internal controls and audit standards.

Key Results (OKRs)

- Maintain **100% audit trail coverage** for critical systems.

- Resolve **≥90%** of ORION[3] Defect Change Backlog items within SLA.

- Execute quarterly context and execution scans[4] across all strategic initiatives.

Measures

- Defect and M&E Change Backlog trends

- Audit compliance pass rate

- Execution scanning scorecard completion

- % of systems with real-time transaction logging

---

[3] Oregon Retirement Information On-Line Network

[4] Context scanning — Focuses on the key internal and external factors that may have an impact on the IT strategy or that may generate risks or issues that the strategy needs to address.

Execution scanning — Focuses on whether the strategy is being executed correctly and whether it is having the expected impact on the enterprise's performance. The metrics defined for each strategic action are one of the main inputs to execution scanning.

Highlighted Measures:

**ORION Maintenance and Enhancement (M&E) Change Backlog**
The Maintenance and Enhancement (M&E) Change Backlog serves as a significant indicator of unresolved application issues reported by the business for enterprise retirement systems. Measured by the number of open ORION M&E Change Records (CR), a growing backlog directly impacts business operations and user experience. Strategic efforts will focus on proactively managing and reducing this backlog, with the current quarterly M&E release cycle remaining a critical lever in achieving this goal.

- ORION Change Backlog: <100 // Trending ↓
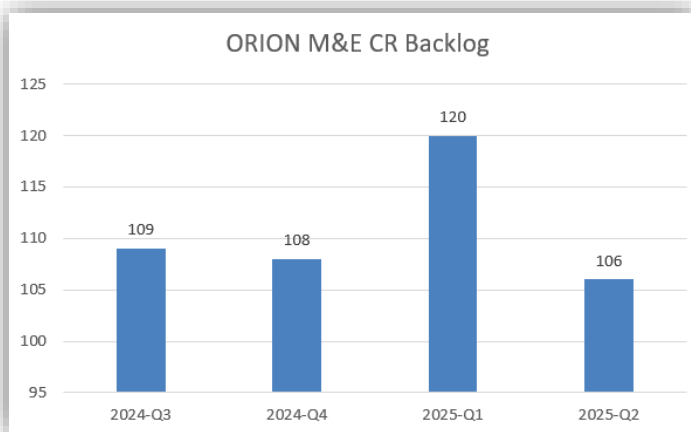
ORION Defect Change Backlog
The Defect Change Backlog represents the accumulation of open ORION defect change records directly related to issues within our enterprise retirement system applications. Reducing this backlog is essential for maintaining system integrity and user satisfaction.

- ORION Defect Backlog: <100 // Trending ↓
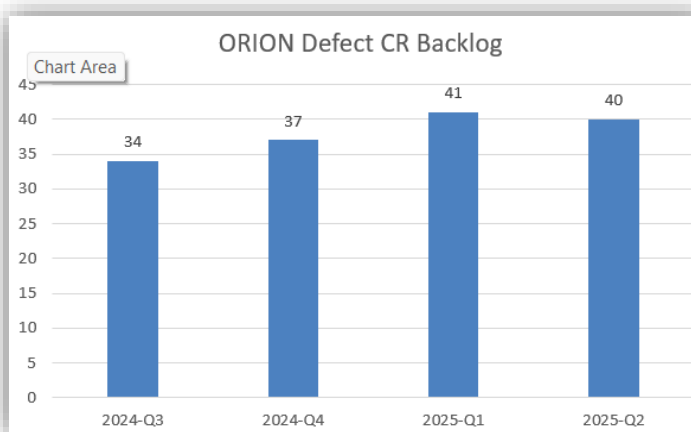
Professional, Accurate, Judicious

Strategic Objective: Deliver reliable, policy-aligned IT solutions that support accurate benefit determination, disbursement, and compliance reporting.

Key Results (OKRs)

- Maintain **<5** batch incidents per month across all production environments.

- Achieve **zero critical calculation errors** per quarter in benefit workflows.

- Document **100% of "as-is" and future-state architecture** for benefit systems.

Measures

- Average batch incidents per month

- Validation error rate in benefit calculations

- Compliance audit findings (none, minor, major)

- Architecture documentation completion rate

Highlighted Measure:

Average batch incidents per month
Average monthly batch incidents directly impact system availability and operational efficiency. The automated batch scheduling system flags incidents upon encountering error codes, potentially causing downtime until resolution. Reducing the frequency of these incidents is crucial for maintaining stable production and minimizing disruptions.

- Avg. batch incidents/month: 1.3
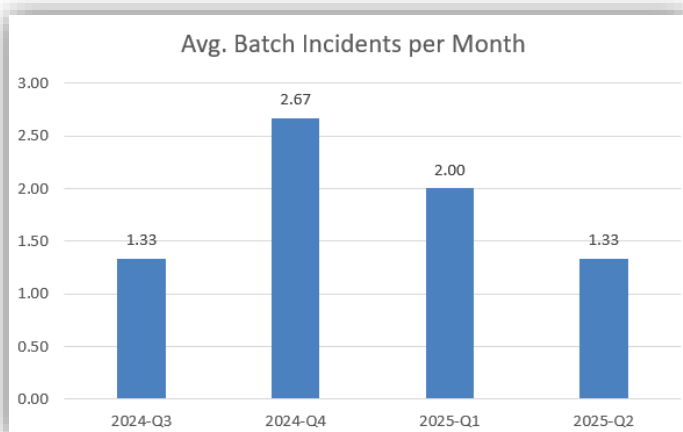
Vigilant

Strategic Objective: Protect member and agency data through layered cybersecurity controls, proactive threat detection, and secure access management.

Key Results (OKRs)

- Achieve **100% patching compliance** for critical systems each quarter.

- Implement MIAM (Member Identity & Access Management) solution by **Q1 2026**.

- Reduce reportable security incidents to **zero per quarter**.

Measures

- Number of security patches deployed vs scheduled

- Progress toward MIAM deployment milestones

- Security incident rate (internal + external)

- Encryption and access control audit results

Highlighted Measure:

Security Incident Rate
The Security Incident Rate tracks the number of reportable internal and external cybersecurity events that compromise, or have the potential to compromise, member or agency data. This metric is a key indicator of the effectiveness of our security posture and the timeliness of threat detection and mitigation efforts. Achieving zero reportable incidents demonstrates strong alignment between our technical controls, monitoring systems, and staff vigilance.

- Zero reportable incidents this quarter

Links to current: Process Measure Scorecard and Operations Measure Scorecard

---

QUARTERLY FOCUS AREA UPDATES

Workforce Development
While technical deliverables did not advance significantly, staff engagement around training needs and modernization awareness continued to grow and efforts advanced to supporting tool and platform selection.

Organizational Communication
Continued support for employee surveys, intranet transition to WordPress, and collaboration tool enhancements to improve internal engagement.

PERS Outcome-Based Management System (POBMS)
PowerBI and Project Web App tools are actively used to report on agency performance and manage project portfolios.

Member Engagement
Follow-up activities from the 2024 Retirement Expo supported ongoing member communication planning.

Omni-Channel Service Delivery
Architecture and planning continued for omni-channel member services, alongside ongoing telephony modernization with Kyndryl and AWS.

Data Analytics
Progressed data cleaning validation in preparation for future platform integration under the Modernization Program.

Data Integrity
Continued defining long-term data cleanup needs to support the future state PAS.

Data Utilization
Ongoing support for the data warehouse and architecture planning for future analytics capabilities.

ORION System Modernization
Provided enterprise architecture input to support ORION planning and its alignment with the broader modernization effort.

Technology Upgrades & System Integration
Maintained support for manual check processes and annual statements while preparing for future automation opportunities.

Financial Management Resource Development
Completed transition of Financial Edge system from on-premise to a cloud-based SaaS environment.

Risk Management System
Planning was revitalized following 2025–27 legislative funding approval.

Information Security Program
Implemented multiple patches and security controls to maintain and strengthen system protection.

Member Privacy
Continued work on the Member Identity and Access Management (MIAM) initiative, supporting secure access infrastructure.

<u>INITIATIVES</u>

The **PERS Modernization Program** remains the largest initiative that the agency is undertaking in support of strategic objectives—choosing to innovate, not just maintain. The agency has made the decision regarding the modernization of the Pension Administration System (PAS) to replace the current system (jClarety) with a Commercial-Off-The-Shelf (COTS) solution.

Efforts at this time primarily involve continuation of documenting current "as-is" architecture, conducting COTS solution evaluation, planning the DevOps roadmap, and collaborating with consultants and subject matter experts for architecture and interoperability assessments.

The **Managed Services Migration** initiative began with Data Center Services (DCS), and preliminary work is complete. However, higher priority projects such as Microsoft Defender and the internet proxy have repeatedly delayed the server migration timeline which could impact system availability and uptime targets.

IT Workforce Development has continued to advance through more assessment of current skills gaps, surveying management and staff, and making further progress in fleshing out the prospective tools to be used and the development plan and schedule.

On the heels of the recently completed Senate Bill 1049, another legislative mandate from **House Bill (HB) 4045 (2024)** - The Police and Fire (P&F) age change component of this bill is scheduled to be implemented by February 2026, and the Hazardous Positions classification must be implemented by January 1, 2030.

Maintenance and operations must continue concurrently with modernization and HB 4045. Initiatives such as the user interface (UI) and user experience (UX) (now collectively referred to as JUMP) will bring the PAS member and employer portal to current standards including Federal compliance to Web Content Accessibility Guidelines (WCAG) 2.1 AA, as well as other legacy stabilization changes planned to provide a solid foundation for modernization.

INITIATIVES DASHBOARD

Initiative	Status	Key Milestones	Risks	Next Steps
PAS Modernization (COTS)	On Track	ODF completed; vendor eval underway	Funding risks, integration complexity	Finalize implementation roadmap (Q4)
Managed Services Migration	Delayed	DCS groundwork complete	Competing priorities (Defender, proxy)	Re-baseline timeline; secure short session funds
IT Workforce Development	On Track	Gap assessment, finalize plan	Resource availability	Launch training pilots (Q1 2026)
HB 4045 Implementation	On Track	Planning underway	Deadline (Feb 2026, Jan 2030)	Confirm scope & schedule with business leads
JUMP UX/UI Modernization	On Track	WCAG review underway	Legacy system constraints	Begin phased rollout design (Q4)

RISKS AND MITIGATION STRATEGY

- Risk #1: New legislation that impacts PERS plans.

  - Mitigation: request budget necessary to implement and address impact to other projects that are in-flight or planned such as HB 4045 and PERS Modernization Program.

- Risk #2: PAS decision for modernization – COTS solution (see details above).

  - Mitigation: request a re-baselined budget in the short session (February 2026).

  - Mitigation: develop contingency planning scenarios for delayed PAS COTS implementation due to potential vendor onboarding delays.

- Risk #3: Delay of managed host migration

  - Mitigation: re-baseline project schedule and request additional budget in short session (February 2026) to cover additional licenses and subscription expenses. May include expenses due to loss of 'warm site'[5] inclusion.

- Risk #4: Emerging technologies – AI

  - Mitigation: monitor AI regulations impacts and CTO perspective with respect to the Oregon IT Enterprise, along vendor dependencies.

- Risk #5: Organizational readiness and change fatigue

  - Mitigation: implement a formal change management framework and strengthen internal communications. Increase investments in training, engagement, and support for impacted staff to ensure adoption and pliability. Monitor organizational readiness through pulse surveys and feedback loops.

NEXT STEPS

1. Finalize PAS modernization (COTS Solution) roadmap, including data migration and contingency plans.

2. Revive support from Data Center Services (DCS) and Resilient Site Infrastructure (RSI) project on Managed Services Migration.

3. Launch change management workstream to support modernization efforts.

---

[5] A warm site refers to a disaster recovery site that is partially equipped with information systems and telecommunications equipment to support operations during a significant disruption.

CONCLUSION

During the past quarter, PERS made significant progress in advancing initiatives aligned with the 2025–2030 IT Strategic Plan. Most notably, the agency finalized the decision to pursue a COTS solution for the future of the Pension Administration System. This marks a pivotal transition from planning to execution and sets the stage for a multi-year modernization effort.

Key developments this quarter included initial scoping and planning activities for the PAS modernization, as well as early preparations for implementation roadmap development. The agency also began foundational work to ensure operational readiness—laying the groundwork for organizational, technical, and cultural change. These efforts are aligned with our focus on improving service delivery, enhancing member experience, and strengthening long-term system resilience.

In addition to PAS-related efforts, the agency achieved important milestones in other strategic areas. These included enhancements to the Telephony system, continued progress on the Hybrid Integration Platform (HIP), and ongoing data cleaning initiatives that support data integrity and readiness. Notably, the Azure Government Community Cloud (GCC) Blueprint received formal approval from the Oregon Department of Administrative Services (DAS), Data Center Services (DCS), and Cyber Security Services (CSS)—a key step in advancing our cloud strategy.

Progress continues to reflect strong cross-functional collaboration and an emphasis on outcome-based success measures. While no major shifts in strategy are recommended at this time, the coming quarters will be critical in validating assumptions, refining timelines, and ensuring that program governance supports sustainable execution.

Overall, PERS remains on track and strategically aligned. Continued monitoring of risks, dependencies, and capacity will be essential as we transition into more active phases of delivery.