Secretary of State
Oregon Audits Division

Public Employees Retirement System

Recommendation Follow-up Report: Progress Made, but Pension Reform Delayed Implementation of Some Recommendations

March 2020
Report 2020-12

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Follow-up to Audit Report 2018-32

Public Employees Retirement System

Recommendation Follow-up Report: Progress Made, but Pension Reform Delayed Implementation of Some Recommendations

March 2020

Follow-up Summary

Oregon's Public Employees Retirement System (PERS) made progress implementing most of the 16 recommendations from the original audit, fully implementing eight. Pension reform legislation, passed in 2019 and otherwise known as Senate Bill 1049, imposed significant responsibilities on PERS. As a result, PERS delayed a number of efforts to address audit recommendations, including developing IT portfolio management, implementing a backup data center, and establishing and testing a comprehensive disaster recovery plan.

Findings from the Original Audit

- PERS's IT strategic planning lacked sufficient detail to help ensure IT investments return the most value, pose the least amount of risk, and are completed timely. Insufficient planning contributed to mismanagement of some agency initiatives.
- The agency's disaster recovery plans posed serious risks because they were not sufficient to restore critical IT systems. Furthermore, the agency had not adequately tested those plans and had not complied with legislative mandates to acquire an alternative recovery site and improve disaster recovery planning. The agency's strategy to re-issue the prior month's payments in the event of disaster increased the risk of benefit payment errors and had never been tested.

Improvements Noted

- PERS's IT strategic plan has been improved and aligned with PERS's enterprise strategic plan. (pg. 2)
- PERS established a backup site geographically distant from the primary site. (pg. 3)
- PERS implemented multiple IT security-related recommendations. (pg. 4)

Remaining Areas of Concern

- PERS has not developed or tested a comprehensive disaster recovery plan. (pg. 3)
- PERS deferred action on IT portfolio management due to pension reform. (pg. 2)

Introduction

The purpose of this report is to follow up on the recommendations we made to the Public Employees Retirement System (PERS) as included in audit report 2018-32, "Severe Deficiencies in Disaster Recovery Program and Insufficient Information Technology Planning Pose Substantial Risks to Beneficiaries and the State."

The Oregon Audits Division conducts follow-up procedures for each of our performance audits. This process helps assess the impact of our audit work, promotes accountability and transparency within state government, and ensures audit recommendations are implemented and related risks mitigated to the greatest extent possible.

We use a standard set of procedures for these engagements that includes gathering evidence and assessing the efforts of the auditee to implement our recommendations; concluding and reporting on those efforts; and employing a rigorous quality assurance process to ensure our conclusions are accurate. We determine implementation status based on an assessment of evidence rather than self-reported information. This follow-up is not an audit, but a status check on the agency's actions.

To ensure the timeliness of this effort, the division asks all auditees to provide a timeframe for implementing the recommendations in our audit reports. We use this timeframe to schedule and execute our follow-up procedures.

Our follow-up procedures evaluate the status of each recommendation and assign it one of the following categories:

- **Implemented/Resolved**: The auditee has fully implemented the recommendation or otherwise taken the appropriate action to resolve the issue identified by the audit.
- **Partially implemented**: The auditee has begun taking action on the recommendation, but has not fully implemented it. In some cases, this simply means the auditee needs more time to fully implement the recommendation. However, it may also mean the auditee believes it has taken sufficient action to address the issue and does not plan to pursue further action on that recommendation.
- **Not implemented**: The auditee has taken no action on the recommendation. This could mean the auditee still plans to implement the recommendation and simply has not yet taken action; it could also mean the auditee has declined to take the action identified by the recommendation and may pursue other action, or the auditee disagreed with the initial recommendation.

The status of each recommendation and full results of our follow-up work are detailed in the following pages.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of PERS during the course of this follow-up work.

Recommendation Implementation Status

Recommendation #1

Develop a detailed IT strategic plan that includes how IT resources will be managed to meet stated objectives.	**Implemented**

The Information Services Division of PERS overhauled its IT strategic plan. PERS's 2018-2023 IT strategic plan includes specific planned actions to achieve agency goals and objectives, such as workforce development and IT resource management. The agency is currently executing the updated plan.

Recommendation #2

Develop and implement a method to track staff time by task or project.	**Not implemented**

In accordance with legislative instructions, the Department of Administrative Services (DAS) and the Office of the State Chief Information Officer (OSCIO) were assigned to provide oversight of the implementation of Senate Bill 1049. Due to the significant workload impacts of the bill and in accordance with directions from DAS and the OSCIO, PERS deferred action on all non-critical IT initiatives, so resources can be applied to implement the legislation. Although PERS is tracking time spent on implementing SB 1049, PERS was directed to put on hold the effort to develop and implement tracking across other projects.

Recommendation #3

Implement comprehensive IT portfolio management including tracking and managing all IT projects and ongoing maintenance efforts.	**Not implemented**

As noted in recommendation no. 2, DAS and the OSCIO directed PERS to place all projects that are not deemed emergent and mission-critical on hold due to the urgency and amount of work associated with SB 1049. PERS's Chief Information Officer reported that the agency intends to pursue IT portfolio management after the implementation of SB 1049.

Recommendation #4

Update documentation around core competencies and skillsets required for the Information Services Division, and clearly define their connection to strategic goals.	**Implemented**

PERS updated its IT strategic plan to include detailed goals and objectives relating to workforce development and their connections to enterprise strategic goals and has updated documentation around core competencies and skillsets required for the Information Services Division.

Recommendation #5

Establish a detailed plan to recruit, train, and retain quality IT staff.	**Partially implemented**

PERS identified a high-level goal to "improve workforce environment and prepare for and attract the next generation of technical talent." Two objectives and five strategies were documented in the updated IT strategic plan. Although PERS initiated a project, specific workforce development action items were deferred, in accordance with directions from DAS and the OSCIO, until efforts around SB 1049 are complete.

Recommendation #6

Develop a process to schedule, track, and allocate sufficient resources to completing the disaster recovery plan.	**Implemented**

Executive leadership receives quarterly updates on disaster recovery and business continuity efforts. PERS management has also prepared a business case to request additional resources to be allocated to these efforts. PERS performed a tabletop test in February 2019 and the disaster recovery plan was updated based on lessons learned from that test. PERS worked to acquire more staffing resources by contracting with several vendors to assist the agency in the effort to implement a backup data center in the cloud.[1] Although a formal disaster recovery resourcing process has not been established, PERS staff noted that the director of the agency has prioritized disaster recovery and business continuity efforts.

Recommendation #7

Ensure the disaster recovery plan reflects short-term and long-term recovery of all critical business systems, including documenting detailed recovery procedures, alternative disaster scenarios, and planned responses.	**Partially implemented**

PERS updated its disaster recovery plan to reflect additional short-term and long-term recovery efforts; however, the existing plans lack critical business needs, such as a solution for restoring the call center, scanning, and restoring IT systems at a backup data center.

Recommendation #8

Establish an alternative backup site that is geographically distant from the primary storage location.	**Implemented**

PERS reported it has established an alternative storage backup site using an Azure Government Tenant cloud storage in Arizona. If PERS loses access to locally stored data backups due to a major disaster, data could be retrieved and restored from the remote site.

Recommendation #9

Establish a disaster recovery warm site as directed by the Legislature.	**Partially implemented**

PERS established a critical project to implement a backup data center (warm site); however, due to SB 1049, this effort was slightly delayed.[2] PERS management hopes to perform go-live testing of the backup data center prior to July 2020. PERS supplemented existing staff with staffing resources from IT contractors.

Recommendation #10

Test the fully developed disaster recovery plan by 2020.	**Not implemented**

---

[1] Cloud computing ("the cloud") is the on-demand delivery of computing services such as servers, storage, databases, networking, and software over the Internet.

[2] There are different types of alternative sites (backup data centers). For example, a cold site is a facility with space and basic infrastructure to support recovery of operations. A cold site takes the most effort and time to recover operations, but is relatively inexpensive. A warm site is a facility with space, basic infrastructure, and all required equipment installed to support recovery of operations. A hot site is a facility with space, basic infrastructure, all required equipment, and all required software installed and running to support recovery of operations. A hot site takes the least amount of effort and time to recover operations, but is also the costliest.

Although PERS updated its existing disaster recovery plan, critical long-term recovery elements of that plan such as scanning, telephone services, and a backup data center have not been completed. In particular, SB 1049 impacted the timeline to complete the backup data center. Following the current disaster recovery plan would not fully restore PERS back to normal operations. Therefore, PERS has been unable to fully test a complete plan. PERS reported performing a tabletop test of the existing plan in February 2019.

Recommendation #11

Improve security management by clearly defining security roles, properly vetting all individuals before granting access to PERS's IT resources, and ensuring that all individuals receive sufficient security awareness training.	**Implemented**

PERS management reported they worked with Cyber Security Services within the OSCIO to establish security roles and responsibilities. The agency also hired additional security staff to perform security compliance functions and established a new process to ensure all employees and contractors undergo background checks. PERS began using statewide security awareness training so staff receive sufficient training and also purchased training for developers on secure software development practices.

Recommendation #12

Remedy weaknesses with Critical Security Control #1 – Hardware Inventory – by further developing written policies and procedures, as well as continuing to mature the application of the new inventory tool.	**Implemented**

PERS updated hardware policies and procedures and continues to mature the application of a hardware inventory tool. The agency performs regular automated hardware scans to identify and inventory all hardware assets.

Recommendation #13

Remedy weaknesses with Critical Security Control #2 – Software Inventory – by further developing written policies and procedures, implementing software whitelisting, and continuing to mature the application of the new inventory tool.	**Partially implemented**

PERS updated software policies and procedures and continues to mature the application of a software inventory tool. The agency performs regular automated software scans to identify and inventory all software assets. Over the next year, management reported they hope to perform additional research to determine the best approach to implement software whitelisting but deferred action at this time.

Recommendation #14

Remedy weaknesses with Critical Security Control #3 – Secure Configurations – through monitoring of configuration changes and by further developing written policies and procedures.	**Implemented**

PERS further developed policies and procedures, including developing a draft policy to respond to compromised machines. PERS also implemented a tool to monitor infrastructure changes.

Recommendation #15

Remedy weaknesses with Critical Security Control #4 – Vulnerability Assessment – by ensuring that known vulnerabilities are tracked and remediated.	**Implemented**

PERS performs regular scans of its network to identify potential vulnerabilities. The agency also developed processes to track and remediate known vulnerabilities.

Recommendation #16

Remedy weaknesses with Critical Security Control #5 – Privileged Access – by implementing improved segregation of duties, monitoring of administrative accounts, and by further developing written policies and procedures.	**Partially implemented**

PERS implemented increased segregation of duties through governance processes as well as multi-factor authentication for privileged user account access. However, minimum password length parameters are still not in full compliance with state security standards. The agency also has plans to implement a privileged access management solution in the future, which should provide increased monitoring and control of administrative accounts. Access policies and procedures have not been updated since the original audit.

Conclusion

PERS made progress toward addressing our recommendations, with eight recommendations fully implemented, five recommendations partially implemented, and three recommendations not implemented.

PERS fully implemented eight recommendations, including developing a new IT strategic plan that is aligned with the agency's strategic plan. The agency also began backing up its data using a cloud-based solution, ensuring the data is maintained at a geographically distant location from the primary data center. PERS also made a number of efforts to fully implement four IT security controls recommendations and has partially implemented the remaining two security-related recommendations.

Pension reform legislation, passed in 2019, delayed action on at least five of our recommendations from the original audit. For example, recommendations no. 2 and 3 were deferred in accordance with instructions from DAS and the OSCIO. Recommendation no. 10, testing a fully developed disaster recovery plan, is dependent on a number of other actions being taken, including implementing a backup data center in the cloud and finding a solution for telephone service and document scanning. This recommendation cannot be implemented until those dependencies are finalized. Without these elements, PERS lacks the assurance needed that the agency can fully restore operations in the event of a major disaster.

Follow-up Report Team

Will Garber, CGFM, Deputy Director

Teresa Furnish, CISA, Audit Manager

Ian Green, M.Econ, CGAP, CFE, CISA, Audit Manager

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits