ERS®
EMPLOYEES RETIREMENT SYSTEM OF TEXAS

Cloud Governance Audit #2023-02 August 23, 2023

From the Director:

Internal Audit has completed its Cloud Governance Audit at the Employees Retirement System of Texas.

Based on the audit scope areas reviewed, the system of internal controls substantially address significant risks. Control gap corrections and improvement opportunities were identified, including:

1) Continue to Mature Cloud Governance (Moderate)

Other matters deemed less significant were communicated to management directly. We thank management and staff of the Information Systems, Office of General Counsel, Office of Procurement and Contracting, Customer Benefits and Investment divisions for their courtesy and cooperation extended to us during the engagement.

Sincerely,

Anthony Chavez

Anthony Chavez, CIA, CGAP, CRMA

Director, Internal Audit Division

ERS Internal Audit Division

Table of Contents

Objectives and Summary Results

Audit Objective: To determine if procedures are in place to ensure cloud management vendors adhere to ERS standards for availability and security.

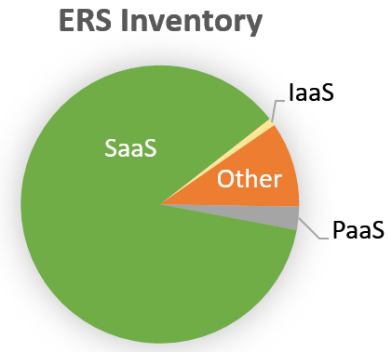
Overall Results: : Internal controls substantially address significant risks related to operational execution. **(Satisfactory)**

SCOPE AREA	SUB-OBJECTIVES	RESULTS/RATING	
Contracting	• Are controls in place to ensure contractual cloud responsibilities are performed by vendor?	Satisfactory	Controls are in place to review key reports on data security and disaster recovery, however improved collaboration is needed. (*See Observation 1)*
Operations	• Are controls in place to determine shared responsibilities based on risks?	Satisfactory	No controls exist to assess each cloud provider for risk, however, the impact to the agency is low as few cloud applications are critical. *(See Observation 1)*

Audit Rating Legend:

Exemplary - Effective, sustainable process	**Satisfactory** - Internal controls effective and working as intended
Needs Improvement - Internal controls partially effective	**Unsatisfactory** - Entire control framework in need of repair

Background

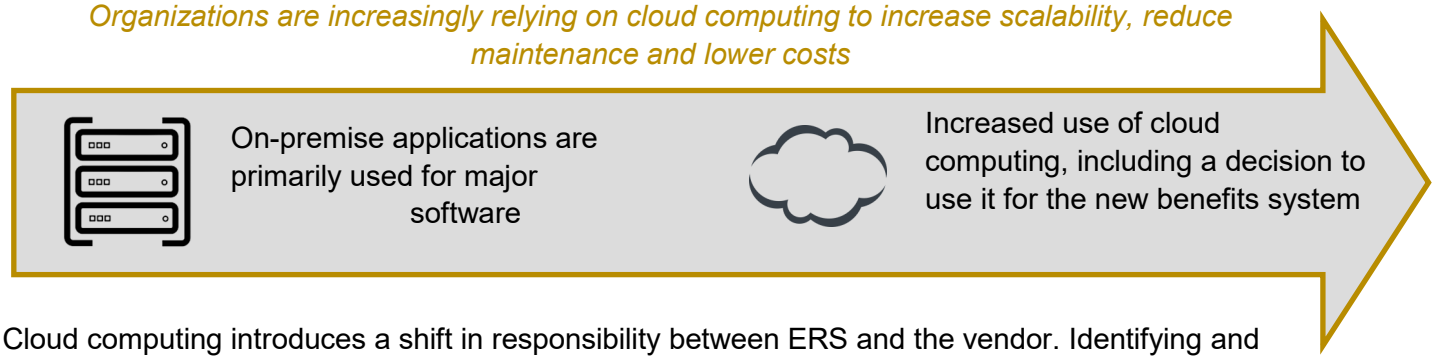


Cloud computing is an on-demand, remote access to information technology (networks, storage, applications, etc.) instead of through on-premise, local infrastructure. There are three service models defined by the National Institute of Standards and Technology (although many sub-models are used by the industry):

- SaaS - Software as a Service
- PaaS - Platform as a Service
- IaaS - Infrastructure as a Service

The 87th Texas Legislature required the Texas Department of Information Security to establish the Texas Risk and Authorization Management Program (TXRAMP) to standardize security assessment, authorization and continuous monitoring of cloud computing services that process the data of state agencies. It also requires state agencies to consider cloud service options for major information system projects or when developing new information technology software applications.

Organizations are increasingly relying on cloud computing to increase scalability, reduce maintenance and lower costs



Cloud computing introduces a shift in responsibility between ERS and the vendor. Identifying and documenting respective responsibilities in the contract is key to effective cloud governance. Using a cloud computing service increases the monitoring activities for the contract manager to beyond performance.

	On Premise	IaaS	PaaS	SaaS
Application configuration	ERS	ERS	ERS	ERS
Identity and access controls	ERS	ERS	ERS / Vendor	ERS / Vendor
Application data storage	ERS	ERS	ERS / Vendor	Vendor
Application	ERS	ERS	ERS	Vendor
Operating system	ERS	ERS	Vendor	Vendor
Network flow controls	ERS	ERS / Vendor	Vendor	Vendor
Host infrastructure, servers, & storage	ERS	Vendor	Vendor	Vendor
Physical security	ERS	Vendor	Vendor	Vendor

ERS is primarily responsible for security

Both ERS and cloud service vendor share security responsibilities

Cloud service vendor is fully responsible for security

Observation 1: Continue to Mature Cloud Governance (Moderate)

Program Risk:	• Agency data subjected to inconsistent and unapproved governance for managing cloud systems • Unauthorized use of cloud based applications create security vulnerabilities and increases risk of data breaches
Inherent Risk:	• On demand, self service model of cloud applications increases risk that applications used without prior approval by Information Services • Reduced visibility into application operations and shared responsibility for mitigating risks in cloud computing • Data deletion is incomplete
Background:	• Cloud governance is a set of policies used by organizations to manage risks around data security, compliance with regulations and overall governance objectives • A governance process should include current documentation of existing cloud services including the business owner, criticality, compliance requirements, and the impact to operations ◦ An inventory can assist with assessing risk and compliance requirements and help prioritize mitigation efforts and determine the level of controls needed for each system • Key controls for cloud applications are reviews of vendor reports on information security and disaster recovery • Cloud applications used by the agency must be obtained through the agency's procurement process which includes varying levels of review based on procurement type (request for proposal, sole source and Texas Department of Information Technology master contracts) • The Texas Government Code mandates that all new or renewed contracts for cloud offerings must meet criteria set by TXRAMP. The implementation date for these criteria is either January 1, 2022, or January 1, 2024, depending on the characteristics of the specific cloud offering • Cloud applications usage at ERS has primarily been for ancillary functions including: news websites, investment and research resources, and collaborative tools

Control Observations:	• Information Systems has commenced the formalization of a comprehensive inventory of cloud computing resources
	• Currently a cloud application risk methodology has not been fully developed to assess information security risk in accordance with ERS Information Security Manual
	• With no fully developed risk rating assessed, information security monitoring plans have not been established for each application. With over 100 cloud applications the level and frequency of vendor report reviews should be targeted for those rated highest risk.
	• The review process for vendor reports on data security and disaster recovery plans (availability) lacks standardization or prioritization. It could not be determined what assurance was provided for current security reviews.
	• A review of four cloud application assessed as higher risk found the following:
	  • For one cloud application assessed as high risk for “Availability”, the full disaster recovery plan and associated test results were not reviewed to ensure alignment with ERS recovery time objectives.
	  • For one cloud application a review of the independent security report was not performed to evaluate risk/impact to ERS at the time of testing and follow-up with vendor to determine corrective actions. A review of the findings by Internal Audit found the impact to be low risk to ERS.

Recommendation:	Information Systems can enhance the cloud governance by performing the following: • Complete the inventory of cloud computing resources • Use that inventory as a basis for assessing cloud applications on an agency-wide basis to identify the most significant applications which may require enhanced monitoring • Collaborate with contract managers and the Office of Procurement and Contracting to add risk attributes meaningful to cloud computing to post-procurement risk assessment • Develop objective criteria for reviewing vendor audit reports for data security and disaster recovery. The criteria should be specific to the contract and enable an assessment that clearly identifies the reviewed aspects and the corresponding results.

Management Action Plan	Management Action Plan: Information Systems agrees with the importance of improving cloud governance, and will complete the following: • Enhancement of procurement processes and forms to provide more detailed guidance and questions to requestors to elicit appropriate determination of the security and availability (disaster recovery) requirements for cloud services. • Establishment of a risk rating methodology for cloud applications, used to determine the level and frequency of the information security and availability monitoring and review for the service and tracked within the cloud application inventory. Responsible Position: Assistant Director of Information Systems Implementation Date: April 1, 2024

Scope and Methodology

We performed this audit in accordance with the FY23 annual audit plan. Internal control activities reviewed include those in place for the ERS Cloud Governance Program from FY20 up to the time of audit fieldwork testing which ended in July 2023.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

A defined set of control objectives was utilized to focus on operational goals for the identified scope. The Committee of Sponsoring Organizations of the Treadway Commission Internal Control Integrated Framework was the basis for internal control assessment. Our Internal Audit opinion is an assessment of the condition of the overall control environment based on the effectiveness of internal control activities through the audit period and the degree to which defined control objectives are being met. Our Internal Audit opinion is not a guarantee of operational effectiveness or regulatory compliance, particularly in areas not included in the scope of this audit.

This audit included a review of internal controls considered relevant to audit objectives including review of statutes, policies and procedures, interviews with management and staff, data analysis and testing procedures.

Related Audits

- 2022-05 Contact Center Audit
- 2022-06 Disaster Recovery Audit
- 2023-01 External Contact Center Audit
- 2023-03 Continuity of Operations Audit

Appendix A: Control Framework

Risk:	Contract managers may not have the expertise to understand
Key Controls:	• The procurement process involves Information Systems staff as a standard procedure in the pre– and post-procurement process • All new systems, regardless of procurement method, are reviewed by Information Systems for compatibility prior to installation

Risk:	Low visibility and oversight of cloud computing by Information Systems
Key Controls:	• Information Systems is formalizing an inventory of cloud computing resources