LACERS
LA CITY EMPLOYEES'
RETIREMENT SYSTEM

Audit Committee Agenda

REGULAR MEETING

TUESDAY, JULY 19, 2022

TIME: 2:30 P.M.

MEETING LOCATION:

In accordance with Government Code Section 54953, subsections (e)(1) and (e)(3), and in light of the State of Emergency proclaimed by the Governor on March 4, 2020 relating to COVID-19 and ongoing concerns that meeting in person would present imminent risks to the health or safety of attendees and/or that the State of Emergency continues to directly impact the ability of members to meet safely in person, the LACERS Audit Committee's July 19, 2022 meeting will be conducted via telephone and/or videoconferencing.

Important Message to the Public

Information to call-in to listen and/or participate:
Dial: (669) 254-5252 or (669) 216-1590
Meeting ID# 160 010 5032

Instructions for call-in participants:

1- Dial in and enter Meeting ID
2- Automatically enter virtual "Waiting Room"
3- Automatically enter Meeting
4- During Public Comment, **press *9** to raise hand
5- Staff will call out the last 3-digits of your phone number to make your comment

Chair:	Elizabeth Lee
Committee Members:	Sung Won Sohn Michael R. Wilkinson
Manager-Secretary:	Neil M. Guglielmo
Executive Assistant:	Ani Ghoukassian
Legal Counselor:	City Attorney's Office Public Pensions General Counsel Division

Notice to Paid Representatives

If you are compensated to monitor, attend, or speak at this meeting, City law may require you to register as a lobbyist and report your activity. See Los Angeles Municipal Code §§ 48.01 *et seq*. More information is available at ethics.lacity.org/lobbying. For assistance, please contact the Ethics Commission at (213) 978-1960 or ethics.commission@lacity.org.

Request for Services

As a covered entity under Title II of the Americans with Disabilities Act, the City of Los Angeles does not discriminate on the basis of disability and, upon request, will provide reasonable accommodation to ensure equal access to its programs, services and activities.

Sign Language Interpreters, Communication Access Real-Time Transcription, Assistive Listening Devices, Telecommunication Relay Services (TRS), or other auxiliary aids and/or services may be provided upon request. To ensure availability, you are advised to make your request at least 72 hours prior to the meeting you wish to attend. Due to difficulties in securing Sign Language Interpreters, five or more business days' notice is strongly recommended. For additional information, please contact: Board of Administration Office at ***(213) 855-9348*** and/or email at ***ani.ghoukassian@lacers.org***.

Disclaimer to Participants

Please be advised that all LACERS Board and Committee Meeting proceedings are audio recorded.

Information to listen only: Live Committee Meetings can be heard at: (213) 621-CITY (Metro), (818) 904-9450 (Valley), (310) 471-CITY (Westside), and (310) 547-CITY (San Pedro Area).

CLICK HERE TO ACCESS BOARD REPORTS

I. PUBLIC COMMENTS AND GENERAL PUBLIC COMMENTS ON MATTERS WITHIN THE COMMITTEE'S JURISDICTION AND COMMENTS ON ANY SPECIFIC MATTERS ON THE AGENDA – *THIS WILL BE THE ONLY OPPORTUNITY FOR PUBLIC COMMENT* - **PRESS *9 TO RAISE HAND DURING PUBLIC COMMENT PERIOD**

II. APPROVAL OF MINUTES FOR THE MEETING OF SEPTEMBER 24, 2019 AND POSSIBLE COMMITTEE ACTION

III. PGOLD VENDOR ASSESSMENT REPORT AND POSSIBLE COMMITTEE ACTION

IV. OTHER BUSINESS

V. NEXT MEETING: The next Audit Committee Meeting is not scheduled at this time and will be announced upon scheduling. Please continue to view the LACERS website for updated information on public access to Board/Committee meetings while response to public health concerns relating to the novel coronavirus continue.

VI. ADJOURNMENT

LACERS
LA CITY EMPLOYEES' RETIREMENT SYSTEM

Board of Administration Agenda

SPECIAL MEETING

TUESDAY, JULY 19, 2022

TIME: 2:30 P.M.

MEETING LOCATION:

In accordance with Government Code Section 54953, subsections (e)(1) and (e)(3), and in light of the State of Emergency proclaimed by the Governor on March 4, 2020 relating to COVID-19 and ongoing concerns that meeting in person would present imminent risks to the health or safety of attendees and/or that the State of Emergency continues to directly impact the ability of members to meet safely in person, the LACERS Audit Committee's July 19, 2022 meeting will be conducted via telephone and/or videoconferencing.

Important Message to the Public

Information to call-in to <u>listen and/or participate</u>:
Dial: (669) 254-5252 or (669) 216-1590
Meeting ID# 160 010 5032

Instructions for call-in <u>participants</u>:

1- Dial in and enter Meeting ID
2- Automatically enter virtual "Waiting Room"
3- Automatically enter Meeting
4- During Public Comment, press *9 to raise hand
5- Staff will call out the last 3-digits of your phone number to make your comment

Information to listen <u>only</u>: Live Board Meetings can be heard at: (213) 621-CITY (Metro), (818) 904-9450 (Valley), (310) 471-CITY (Westside), and (310) 547-CITY (San Pedro Area).

President:	Vacant
Vice President:	Sung Won Sohn
Commissioners:	Annie Chao Elizabeth Lee Sandra Lee Nilza R. Serrano Michael R. Wilkinson
Manager-Secretary:	Neil M. Guglielmo
Executive Assistant:	Ani Ghoukassian
Legal Counsel:	City Attorney's Office Public Pensions General Counsel Division

Notice to Paid Representatives

If you are compensated to monitor, attend, or speak at this meeting, City law may require you to register as a lobbyist and report your activity. See Los Angeles Municipal Code §§ 48.01 *et seq*. More information is available at ethics.lacity.org/lobbying. For assistance, please contact the Ethics Commission at (213) 978-1960 or ethics.commission@lacity.org.

Request for Services

As a covered entity under Title II of the Americans with Disabilities Act, the City of Los Angeles does not discriminate on the basis of disability and, upon request, will provide reasonable accommodation to ensure equal access to its programs, services and activities.

Sign Language Interpreters, Communication Access Real-Time Transcription, Assistive Listening Devices, Telecommunication Relay Services (TRS), or other auxiliary aids and/or services may be provided upon request. To ensure availability, you are advised to make your request at least 72 hours prior to the meeting you wish to attend. Due to difficulties in securing Sign Language Interpreters, <u>five</u> or more business days' notice is strongly recommended. For additional information, please contact: Board of Administration Office at ***(213) 855-9348*** and/or email at ***ani.ghoukassian@lacers.org***.

Disclaimer to Participants

Please be advised that all LACERS Board and Committee Meeting proceedings are audio recorded.

CLICK HERE TO ACCESS BOARD REPORTS

I. PUBLIC COMMENTS AND GENERAL PUBLIC COMMENTS ON MATTERS WITHIN THE COMMITTEE'S JURISDICTION AND COMMENTS ON ANY SPECIFIC MATTERS ON THE AGENDA – *THIS WILL BE THE ONLY OPPORTUNITY FOR PUBLIC COMMENT* - **PRESS *9 TO RAISE HAND DURING PUBLIC COMMENT PERIOD**

II. APPROVAL OF MINUTES FOR THE MEETING OF SEPTEMBER 24, 2019 AND POSSIBLE COMMITTEE ACTION

III. PGOLD VENDOR ASSESSMENT REPORT AND POSSIBLE COMMITTEE ACTION

IV. OTHER BUSINESS

V. NEXT MEETING: The next Audit Committee Meeting is not scheduled at this time and will be announced upon scheduling. Please continue to view the LACERS website for updated information on public access to Board/Committee meetings while response to public health concerns relating to the novel coronavirus continue.

VI. ADJOURNMENT

MINUTES OF THE REGULAR MEETING
AUDIT COMMITTEE
BOARD OF ADMINISTRATION
LOS ANGELES CITY EMPLOYEES' RETIREMENT SYSTEM

LACERS Ken Spiker Boardroom
202 West First Street, Suite 500
Los Angeles, California

September 24, 2019

9:06 a.m.

Agenda of: <u>July 19, 2022</u>
Item No: <u>II</u>

PRESENT:	Chair:	Elizabeth Lee
	Committee Member:	Michael Wilkinson
	Manager-Secretary:	Neil M. Guglielmo
	Executive Assistant:	Ani Ghoukassian
	Audit Manager:	Rahoof “Wally” Oyewole
	Legal Counselor:	Anya Freedman Joshua Geller
ABSENT:	Committee Member:	Sung Won Sohn

The Items in the Minutes are numbered to correspond with the Agenda.

I

PUBLIC COMMENTS ON MATTERS WITHIN THE COMMITTEE’S JURISDICTION – Chair Elizabeth Lee asked if any persons wished to speak, to which there was no response and no public comment cards were received.

II

APPROVAL OF MINUTES FOR THE AUDIT COMMITTEE MEETING OF MAY 14, 2019 AND POSSIBLE COMMITTEE ACTION – A motion to approve the Minutes was moved by Committee Member Wilkinson, and adopted by the following vote: Ayes, Committee Member Wilkinson and Chair Elizabeth Lee -2; Nays, None.

III

AUDIT ACTUARY FINALIST PRESENTATIONS AND POSSIBLE COMMITTEE ACTION – Rahoof “Wally” Oyewole, LACERS Departmental Audit Manager, presented this item to the Committee. Representatives from Milliman and Cheiron, Inc. presented to the Committee. Committee Member Wilkinson moved to recommend Cheiron, Inc. to the Board for contract award to perform the audit actuary engagement , and adopted by the following vote: Ayes, Committee Member Wilkinson and Chair Elizabeth Lee -2; Nays, None.

IV

UPDATE FROM BROWN ARMSTRONG ACCOUNTANCY ON THE AUDIT OF LACERS FINANCIAL STATEMENTS FOR THE YEAR ENDED JUNE 30, 2019 - Rahoof "Wally" Oyewole, LACERS Departmental Audit Manager and via phone Rosalva Flores, CPA with Brown Armstrong, presented this item to the Committee.

V

OTHER BUSINESS – There was no other business.

VI

NEXT MEETING: Chair Elizabeth Lee announced that the next Audit Committee Meeting is not scheduled at this time, and will be announced upon scheduling.

VII

ADJOURNMENT: There being no further business before the Committee, Chair Elizabeth Lee adjourned the Meeting at 10:05 a.m.

____
Elizabeth Lee
Chair

____
Neil M. Guglielmo
Manager-Secretary

REPORT TO THE AUDIT COMMITTEE **MEETING: JULY 19, 2022**
From: Maria Melani Rejuso, Departmental Audit Manager **ITEM: III**
Maria Melani Rejuso

SUBJECT: **PGOLD VENDOR ASSESSMENT AND POSSIBLE COMMITTEE ACTION**

ACTION: ☒ CLOSED: ☐ CONSENT: ☐ RECEIVE & FILE: ☒

Recommendation

That the Audit Committee:

1. Receive and file the "PGold Vendor Assessment Report (Report)" issued by LACERS Internal Audit in partnership with Grant Thornton, LLP.

2. Consider and/or approve the Report's recommendations to improve the Retirement System application's controls, benefit processes, and users experience.

Executive Summary

Internal Audit's last risk assessment, conducted during FY2021, identified potential areas of risks related to LACERS Information Technology Systems that can compromise the department's data, information, and assets.

One risk area that stood out was LACERS retirement system application (PGold). Specifically, there were growing concerns from management and users on the safety of members' information triggered by the increasing reports on data compromise incidents, in both private and public sectors.

To mitigate this risk, Internal Audit initiated a PGold Vendor audit to evaluate the following control areas:

- Segregation of duties
- Documented and applied policies and procedures
- Acquisition, development, and change-control practices
- Database administration practices
- Production control practices
- Access and transaction authorizations, and
- Monitoring practice

The audit was carried out in partnership with Grant Thornton, LLP, a subject matter expert in auditing information technology systems. This is part of a series of information technology-related audits we contracted with Grant Thornton, LLP.

The primary purpose of this audit was to evaluate the adequacy and effectiveness of the control framework embedded into LACERS retirement system application, called PGold (PensionGold version3). PGold maintains the members employment and benefits information. It was developed and sold by LRS (vendor) and is currently the service provider for this application.

Discussion

The results of the assessment audit identified areas that are working and those that need improvement.

The audit found that the following control areas in PGold are ***working:***

- LACERS has a process in place to manage user authentication and authorization in PGold.
- LRS ensures its in-house architects and developers follow secure coding practices by having recurring training on secure coding, doing automated scanning and code reviews, and requiring management approvals for code creation/changes.
- Both LRS and LACERS identify, track, and remediate vulnerabilities in the application. For example, LRS performs vulnerability scanning during code creation as well as base application penetration testing before deploying the codes into the application environment. On the other hand, LACERS uses Symantec to continuously scan PGold and its environment.
- LACERS' SOS team and the requestor section test the updates/fixes before deploying them into the production. Similarly, LRS performs testing at various stages of the software development lifecycle before moving them to production.
- LRS ensures that access to the server where data is stored (within PGold) is segregated from LRS staff responsible for application code development. Similarly, LRS staff working in the code development environment are separated from those LRS staff working in the test environment. LRS does not use contractors for code development

The audit found that the following control areas in PGold ***need improvement:***

For LRS, including future maintenance agreement:

- Lack of controls to manage instances where service response timeframes were not met by LRS. Future maintenance agreement should include provisions on consequences or penalties (e.g., financial remedies, license/support extension) when timeframes are not met.

- LRS does not provide sufficient information about updates on PGold. LRS should ensure that all PGold updates are fully disclosed with LACERS.

- Future maintenance agreement should include descriptions of what qualifies as emergency, non-emergency, or enhancements. Also, descriptions should be consistent with the priority/severity levels shown in the sharepoint portal. Currently, the portal shows a numeric priority or severity levels 1 to 3, which is not consistent with the maintenance agreement.

- Keep software development workflow documentation updated to reflect the current environment. For example, the development workflow described in the maintenance agreement states that LACERS developers are responsible for application codes. LACERS does not have in-house developers and this function has been given up to LRS as a control measure.

Improvement Opportunities for LACERS Business Users (LACERS staff)

- Ensure all business users are aware of any changes in the application that may affect their subsequent use of the system. LACERS should have a cross-functional improvement team consisting of representatives from each business unit to discuss application changes and deployed changes.

- LACERS should organize employee users into focused security groups to help streamline access for certain job functions, while narrowing the scope of permissions to specific data. The process should include defining the group members roles and functions (including approval requirements).

- LACERS should perform recurring access reviews or recertifications to ensure each level of access is appropriate to staff job duties, especially for users who transfer to different teams.

- LACERS should work with LRS to completely mask or gray out Personally Identifiable Information (PIIs), e.g., SSN, birthdates, hire dates, etc. in PGold. Access to these PIIs should be limited for certain uses (e.g., verification, audit).

- LACERS should review the security controls of newly developed applications (ancillary systems) like MyLACERS before deploying them into the environment for use.

- Long standing or Open Problem Incident Reports (PIRs). LACERS should work with LRS to completely close out incident cases initiated in the sharepoint portal. A number of PIRs are still outstanding and have not been closed out. An example of this is related to payroll reporting updates.

- LACERS should track the PIR trends (reasons and resolution timeliness) to understand the effectiveness and efficiency of the application sold by LRS and the quality of service being provided by LRS. This is particularly important when negotiating for a new contract.

- Although access and maintenance of application codes resides with LRS (which is a good control), it is also a good practice to allow LACERS to have a “read-only” access of codes activities to keep LACERS staff aware of any changes in the application codes, particularly those not initiated by LACERS.

- LACERS should implement a process to have duplicate or incorrect information in PGold deleted as business users become aware of it. Per LRS, data clean up can be requested by LACERS staff through the PIR system.

Details of the issues described above are discussed fully in the attached audit report. The issues were discussed with LRS and LACERS staff (SOS, PGold Systems, Executive Officer), and they agreed to implement the related recommendations. The implementation plan will be submitted by LACERS after the issuance of this report.

Prepared By: Maria Melani Rejuso, Departmental Audit Manager

MR/NMG/mr

Attachment: PGold Vendor Assessment

Grant Thornton

LA City Employees Retirement System (LACERS)

PGold Vendor Assessment

Detailed Risk Assessment Report

July 19, 2022

Table of Contents

Executive Summary

Background and Objectives 3

Approach 4

Executive Report Summary 5

Current State Program Highlights 6

Improvement Opportunities Reported by LACERS Business Users 7

LRS Improvement Opportunities 8

Suggested LRS Contract Enhancements 9

Additional Process Improvement Opportunities (To be Considered by LACERS) 10

Detailed Report

Appendix A – Detailed Assessment Report 11 - 18

Appendix B – Control Strengths 19-21

Appendix C – Stakeholders 22-23

© 2022 Grant Thornton LLP | All rights reserved

Background and Objectives

❑ Evaluate the adequacy and effectiveness of the control framework embedded into the Retirement System Application Pension Gold version 3 (PGoldV3) as developed by Levi, Ray & Shoup Retirement Services (LRS).

❑ Provide an independent assessment of the service provider's quality of service and compliance with their contract and maintenance agreement with Lacers. This includes evaluation of select IT controls as given below:

- Segregation of Duties
- Documented and applied policies and procedures
- Software Development Lifecycle and Change control
- Database Administration practices
- Production control practices
- Access management
- Monitoring practices

© 2022 Grant Thornton LLP | All rights reserved

Approach

	Phase 1	Phase 2	Phase 3
	Perform current state vendor risk assessment	**Evaluate adequacy and effectiveness of control framework**	Develop an executive report on LACERS’ current state of vendor managing PGoldV3
Key Activities	• Obtain an understanding of LACERS’ reliance on a third party for a critical system. • Obtain an understanding of processes within the Retirement System through review of documentation supporting current state of LACERS’ version of Pension Gold software.	• Measure the service provider’s level of security and its ability to adequately address emerging cyber security risks. • Provide recommendations based on industry best practice pertaining to third party management for those areas where improvements are identified.	• Develop an executive report, providing key findings that specify process improvements to vendor software administration based on industry leading practices (MS PowerPoint). • Assist LACERS’ IT team to present the vendor assessment results to the LACERS’ Audit and Compliance Committee, if needed.
Outcomes	• Audit plan and assessment framework • Kick off meeting • Document request list	• Completed gap assessment • Prioritized recommendations	• Executive audit report • Communication with senior leadership

© 2022 Grant Thornton LLP | All rights reserved

Executive Report Summary

The assessment focused on evaluating LACERS' vendor supplied Retirement System Application, Pension Gold version 3 (PGoldV3), against vendor contract and compliance documentation to identify control gaps and process improvement opportunities.

Current State Program Highlights

The following represents an overview of the PGoldV3 application and key areas of improvement that were noted.

- ❖ **Access Control.** LACERS has an established access management process that incorporates the principle of least privilege and is facilitated through the PGoldV3 Security Console and Active Directory.
- ❖ **Security Training.** On a regular basis, LRS architects and developers complete secure code training. In addition, LACERS performs periodic social engineering/phishing campaigns.
- ❖ **Vulnerability Scanning.** LRS performs vulnerability scanning of their environment and application code during the development and testing processes to identify, track, and remediate internal and external vulnerabilities. LACERS also performs vulnerability scanning.
- ❖ **Application Security Testing.** LACERS and LRS both conduct testing at various stages of application development for updates/fixes prior to deploying them into production.
- ❖ **Segregation of Duties**. LRS segregation of duties controls adequately manage risk across the Software Development Lifecycle and are in line with industry standards and best practices.

See page 6 for more details

LRS Improvement Opportunities

Based on GT's assessment, GT recommends management enhance the following areas which will help LACERS' application functionality.

- ❖ While there were no instances found where LRS did not meet Service Level Agreements (SLA), there are limited controls in place to manage instances in case SLA timeframes are not met while responding to or completing Problem Incident Reports (PIRs). Such controls may include but not limited to financial compensation, service credits, or extension of support services.
- ❖ LRS does not consistently include sufficient information on updates that are performed for PGoldV3. LACERS should request that, in addition to the information that is included in the Problem Incident Report (PIR) notes, LRS provide more detailed information about each PGoldV3 update that is completed and LRS should obtain from LACERS acknowledgement of closure of fixes.
- ❖ Within the contract agreement, the software development lifecycle workflow diagram does not accurately depict the current environment to illustrate how the application versions and updates of software are deployed.

See page 8 for more details

© 2022 Grant Thornton LLP | All rights reserved

Current State Program Highlight Details From page 5

Based on GT's assessment through workshops and review of supporting documentation provided, the following are highlights of LACERS' and PGoldV3 vendor (LRS) strengths, including:

Access Controls have been established. Administered by LACERS, access permissions within PGoldV3 is performed using a central security console within PGoldV3. When needed, LRS access is granted and revoked in real-time and performed by LACERS' SYS group. Active Directory is used to manage access within the application by using security groups assignable within the PGoldV3 security console. As noted in the cybersecurity assessment, the **access management process incorporates principal of least privilege, requires appropriate approval, includes annual recertification and all access is facilitated and tracked** through the Numara helpdesk/ticketing system.

Recurring training for secure application code is performed. **LRS requires training for each job function such as architect, developer, etc as well as regular in-house secure code training**. Code review takes place at several intervals, including peer-review and management approvals to ensure secure code practices are carried forward.

Vulnerability scanning and penetration testing is performed. Vulnerabilities are identified, tracked, and remediated by both parties. **LRS performs regular vulnerability scanning during code creation and base application penetration testing is also performed prior to deployment**. All scan reports are loaded into the PGoldV3 portal for LACERS' review. Internally, LACERS uses Symantec to continuously scan the application and their environment.

LACERS' SOS team coordinates application testing. **Application testing, facilitated by LACERS' SOS team, is conducted by affected user groups for all PGoldV3 updates/fixes prior to deploying them into the production environment**. Additionally, LRS performs testing at various stages of the software development lifecycle including prior to code package moving from development to test and after test environment before moving to production.

LRS Segregation of duties and peer reviews. **LRS utilizes a multi-layered approach designed to strengthen segregation of duties.** LRS employs both a sequential level and individual level technique to separate duties with respect to 1.) access to the server where LACERS data is stored, and 2.) application code development. Access is only available to LRS employees (contractors are not permitted access) who are members of the software development team and developers working in the development environment are segregated from those working in the test environment. Code development requires a peer review at both data conversion and code development stages and code at all stages require manager approval before advancing.

© 2022 Grant Thornton LLP | All rights reserved

Improvement Opportunities Reported by LACERS Business Users

Based on workshops with various groups within LACERS, the following process and control improvement opportunities about PGoldV3 were noted, including:

Awareness of application changes. Business Users reported that they are not notified / informed of changes made to the application and how it will impact their groups. For example, when a Problem Incident Report (PIR) is completed, the initiator may be satisfied by testing the changes. However, when implemented, those changes could affect downstream users and if those downstream users are not notified of the impact, depending on the changes, they may not be able to perform their job duties in the same manner.

Business Groups have inappropriate access. Business Users reported that some have access to certain screens or data fields that they should not have access to. During discussions, it was noted that a LACERS employee from one group sent documentation to a pension member but should not have had the ability to do so. It was also noted that some LACERS employees have inappropriate read or write access.

MyLacers user was able to gain access to another user's account. Business User reported a concern about application security after a user was able to obtain access to another user's account. After review of the Problem Incident Report (PIR), Security Incident Report and discussion with LACERS and LRS, the specific situation was considered as an improvement opportunity to enhance application security.

Long-standing open Problem Incident Reports (PIRs). Inadequate controls over time periods defined to close PIRs. LACERS users noted that critical PIRs, such as payroll reporting updates, which are not resolved and closed in a reasonable period can negatively impact the reliability and/or efficiency of the PGoldV3 application.

Data clean-up opportunities. Business users reported a **need to clean up duplicate and incorrect account information** in PGoldV3. LACERS should consider implementing a process to have employees submit a request to delete incorrect account information as they become aware of it.

© 2022 Grant Thornton LLP | All rights reserved

LRS Improvement Opportunities From page 5

Based on GT's assessment and review of supporting documentation provided, the following are areas of process improvement for LRS regarding PensionGoldV3:

Documented Policies and Procedures:

LACERS should work with LRS to:

- Update Problem Resolution Procedures within the maintenance agreement to include language clarifying consequences or penalties (e.g., financial remedies, license, or support extension, etc.,) within the future SLA for instances when timeframes are not met.
- Add more detailed explanations around Problem Incident Report (PIR) priority and severity including how those classifications are determined. For example, the priority in the SharePoint portal is numeric (1 through 3) and in the maintenance agreement, it is descriptive ("emergency", "non-emergency", "enhancement").
- Keep software development workflow documentation detailed in the contract to reflect the current environment and be updated/amended as changes are made, not until the expiration of the contract.

Acquisition, development and change-control:

LACERS should work with LRS to:

- Consider revising the Service Level Agreement timeframes. Currently, the agreement states the timeframes for emergency Problem Incident Reports (PIRs) are 2 days to fix the issue and 180 days to close the service ticket. Per review of documentation provided, emergency PIRs are being fixed within 2 days, however, LACERs should consider reducing the timeframe to close emergency tickets. Leading practices recommend closing emergency change requests within 30 days in order to avoid vulnerabilities from being exploited. Timeframes from the Service Level Agreement should be included in the SharePoint portal to ensure necessary updates to the application take place according to the Service Level Agreement.

Access and Transaction Authorizations:

LACERS should work with LRS to:

- Maintain an inventory list of the fields LACERS considers having sensitive information (e.g., SSN, DOB) that require additional level of protection. LACERS would submit a PIR to request these fields be protected (i.e., grayed out).

© 2022 Grant Thornton LLP | All rights reserved

Suggested LRS Contract Enhancements

Based on GT's assessment and review of supporting documentation provided, the following are suggestions of enhancements to the contract with LRS regarding PensionGoldV3:

Service Level Agreement:

- Problem Resolution timeline objectives should be revisited. E.g., The current maintenance requirements on page 5 of the contract for emergency problems require closure (which means providing final corrections, revised License Software and documentation) within 180 days by LRS. Industry leading practice recommends 30 days to close critical (emergency) change requests.
- Service Level Agreement (SLA) procedures, within the maintenance agreement extension of the current contract, do not have clearly defined metrics. E.g., The priority level in the SharePoint portal is a numeric scale 1-3 (where PIRs are recorded). However, in the contract it is descriptive "emergency", "non-emergency" and "new feature/enhancement" with no clear indication of how 1 - 3 numeric values are related to emergency enhancements. Consider adding a risk priority definition that takes into consideration the Impact and Likelihood that together provides a risk priority on a scale of 1-3 (High, Medium, Low).
- There is lack of clarity on how service levels are verified: Where metrics are derived from and what consequences or penalties are in place for instances if/when service level expectations are not met (e.g., License or support extension of 1 week for delayed resolution, 0.25% of payment refund for every 2 hours delay in resolution capped at 15%, etc.)?

Software Development Lifecycle:

- Workflow documentation should always depict the current environment. The current contract incorrectly illustrates the Software Development Lifecycle process which includes a LACERS developer using a Virtual Private Network to access the server on the LRS network in order to create and promote code. It was noted that LACERS does not have developers on staff who write code.

© 2022 Grant Thornton LLP | All rights reserved

Additional Process Improvement Opportunities (To be Considered by LACERS)

Based on GT's assessment and review of supporting documentation provided, the following are areas of process improvement for LACERS regarding PensionGoldV3:

- **Performing recurring access reviews/recertifications** of all users ensures each level of access is appropriate to their job duties; especially for users who transfer to different teams. Also, using more focused security groups can help streamline access for certain job functions within teams and narrow scope of permissions by limiting access to specific data.
- LACERS should **organize employee users into focused security groups to help streamline access for certain job functions** while narrowing the scope of permissions by limiting access to specific data. All access, whether administrator, generic or unique user accounts should be controlled by one central authority. Additionally, all user accounts including privileged, service, and generic accounts should be controlled by a central authority.
- LACERS should develop and implement a policy regarding personally identifiable information (PII) and how the application treats such data. Work with LRS through the PIR process to mask or gray out the data fields based on business requirements. LACERS employee users noted PII should be made unavailable after they are logged in. This would be done by opening a PIR to mask or gray out the data fields requested.
- **An application owner within LACERS should regularly obtain the status from the PGoldV3 portal regarding vendor deployment updates and share with all applicable users**. Create and distribute application roles and responsibilities, resources, and user functionality suggestions/updates to share information with users across the organization. The SOS group has a good foundation of this with their documentation and the LRS contract and SOC 2 provide details about the shared responsibility model between LRS and LACERS.
- **LACERS should track PIR trends regarding reason and resolution timeliness** to monitor vendor service levels, keep employee users informed and organize workload. Work with LRS to escalate completion of existing PIRs to enable multifactor authentication.
- LACERS should **develop sufficient documentation describing application updates performed for PGoldV3** including why the update is taking place (i.e., response to security defect or incident, regular version control, feature upgrade, etc), what and where specific changes the organization will observe within the application, and shared with all downstream users, even those not directly connected to the specific PIR.
- LACERS may benefit by **implementing a cross-functional improvement team consisting of representatives from each business unit to discuss application issues, deployed changes,** and other nuances of the PGoldV3 system to improve awareness of functionality. Regularly held workshops might also help share ideas, keep personnel informed of recent changes and upcoming releases and other nuances of the Pension Gold system to improve user functionality.

Grant Thornton

Appendix A

Detailed Assessment Report

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations Summary

Assessment Categories	Number of observations for LRS	Risk Level	Recommendation	Number of observations for LACERS	Risk Level	Recommendations
Access and transaction authorizations	1	High	Mask PII data fields. See page 13.	1	High	One central authority, use narrow user security groups, perform user recertifications. See page 16.
Acquisition, development and change-control practices	1	Low	SLA metric in portal. See page 15	None	NA	NA
Documented and applied policies and procedures	2	Med/ Low	PIR SLA definitions. SDLC workflow. See page 14.	1	High	Develop sensitive data policy. See page 17.
Segregation of Duties (SOD)	None	NA	NA	None	NA	NA
Database Administration practices	None	NA	NA	1	High	Restrict data fields with PII. See page 16.
Monitoring practices	None	NA	NA	2	Med/ Low	Assign application owner and implement cross-functional team. See page 17/18.
Production Control Practices	None	NA	NA	1	Low	Create production documentation for users across the enterprise. See page 17.

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LRS

Assessment Categories	Observation	Risk Level	Recommendations	Management Action Plan
Access and transaction authorizations	Ob-1. As a result of the Problem Incident Resolution & Security Incident Report as noted on page 7, it was noted that business requirements regarding data fields containing sensitive information and requiring added security measures are not managed.	High	LACERS should request LRS to maintain a list of fields that LACERS deems “sensitive information” that demands an additional layer of protection against disclosure or corruption.	

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LRS

Assessment Categories	Observations	Risk Level	Recommendations	Management Action Plan
Documented and applied policies and procedures	Ob-2. The established maintenance policy that includes Service Level Agreements (SLAs) regarding timeframes for acknowledging resolution and completion of Problem Incident Reports (PIRs) does not include outcomes or remediation efforts for instances when SLAs are not met, adequate timeframes for emergencies or specific descriptions of PIR classifications.	Med	LACERS should request LRS to update their Problem Resolution Procedures within the maintenance agreement to include: language clarifying consequences or penalties (such as financial remedies, license or support extension, etc) within the future SLA for instances when timeframes are not met, detailed explanations around PIR priority and severity including how those classifications are determined, and more realistic timeframes especially for emergencies.	
	Ob-3. Current contract documentation indicates the LACERS developer accesses the LRS network through VPN to pull code from the Team Foundation DEV Server and processes code through to TEST through package release to LRS. After discussion, IA noted that this does not accurately depict the current environment which includes LRS writing all DEV code and LACERS is engaged after LRS pushes package to their PROD server.	Low	LACERS should request LRS to update application software development workflow documentation detailed in the contract to always reflect the current environment and be updated/amended as changes are made; not at the expiration of the contract. Workflow documentation illustrating the development lifecycle of the software, should include how the base application versions, deployed features, and defect updates of software are installed through the various stages of code development, test and production including meticulous procedures regarding software package transfer from LRS to LACERS.	

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LRS

Assessment Categories	Observation	Risk Level	Recommendations	Management Action Plan
Acquisition, development and change-control practices	Ob-4. Documented acknowledgement and resolution plan(s) for PIRs is performed through the SharePoint portal. The acknowledgement metric within the service level agreement (either 1, 2 or 10 days from the Open Date; depending on the priority) is reliant on the SharePoint portal field "LRS Planned Resolution" notes including a date.	Low	LACERS should request LRS to add a data category in the portal that automatically calculate the service level agreement metrics as detailed in the maintenance agreement.	

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LACERS

Assessment Categories	Observation	Risk Level	Recommendations	Management Action Plan
Access and transaction authorizations	Ob-1. A shared security model is established between LRS and LACERS regarding access rights. Within LACERS, the PGold security console permits isolation of users and groups of users to specific software components, such as webpages, jobs, reports, menus, and embedded hyperlinks. Several groups within LACERS make updates to various types of user access allowing users access to data that they should not have access to.	High	R-1. LACERS should organize employee users into focused security groups to help streamline access for certain job functions while narrowing the scope of permissions by limiting access to specific data.	
		High	R-2. All access, whether administrator, generic or unique user accounts should be controlled by one central authority.	
		High	R-3. Performing recurring access reviews/recertifications of all users ensures each level of access is appropriate to their job duties; especially for users whose roll within the company changes.	
Database Administration Practices	Ob-2. LACERS users are concerned that users have access to certain screens or data fields that they should not have access to. During workshops, it was noted that a LACERS employee sent documentation to a pension member, but their role should not have had the ability to do so.	High	R-4. LACERS should work with LRS through the PIR process to restrict certain fields making the data not accessible to specific user security groups to eliminate inappropriate or accidental changes.	

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LACERS

Assessment Categories	Observation	Risk Level	Recommendations	Management Action Plan
Documented and applied policies and procedures	Ob-3. During workshops, it was noted that some users who appropriately have access to specific screens still should not see fully disclosed PII. Additionally, employee users noted PII should be made unavailable after they are logged in.	High	R-5. LACERS should develop and implement a policy regarding personally identifiable information (PII) and how the application treats such data.	
Monitoring Practices	Ob-4. A PGoldV3 application owner was not identified as responsibility for the application is distributed among multiple groups.	Med	R-6. LACERS should assign an application owner to track PIR trends for reason, resolution timeliness, monitor vendor service levels, keep employee users informed, and organize workload. The owner should also work with LRS to escalate completion of existing PIRs to enable multifactor authentication.	
Production Control Practices	Ob-5. During workshops, it was noted that some users are unaware of changes made to the application or the reason their screens appear different or require a change to their day-to-day processes.	Low	R-7. LACERS should develop documentation describing all application updates within PGoldV3 including why the update is taking place (i.e., response to a security defect or incident, regularly scheduled version control, requested feature upgrade, response to specific PIR, etc), what and where specific changes the organization will observe within the application, and share with all downstream users, even those not directly connected to the specific PIR.	

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Improvements and Recommendations - LACERS

Assessment Categories	Observation	Risk Level	Recommendations	Management Action Plan
Monitoring Practices	Ob-6. Throughout the engagement, it was noted that several users among all groups were not clear of PGoldV3 roles and responsibilities, deployed changes made to the application, how changes are communicated, and pending PIRs.	Low	R-8. LACERS should implement a cross-functional team consisting of representatives from each business unit to collectively discuss PGoldV3 issues, deployed changes, and other nuances of the system to improve awareness and functionality. Regularly held workshops might also help share ideas among users, keep all personnel informed of efficiencies, recent changes, upcoming releases, and other nuances of the Pension Gold system to improve user functionality.	

© 2022 Grant Thornton LLP | All rights reserved

Grant Thornton

Appendix B

Detailed Assessment - Control Strengths

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Strengths

Assessment Categories	Current Process	Result
Segregation of Duties (SOD)	LRS employs both sequential and individual separation of duties techniques with respect to 1.) access to the server where LACERS data is stored, and 2.) application code development. Access is only available to their employees (contractors are not permitted access) who are members of the software development team that have a need to know. Secure code peer reviews are performed at different gates including data conversion and code development. Additionally, developers working in the development environment are segregated from those working in the test environment. Artifacts from both teams are approved by a manager before code moves to the next stage. Finally, audit logging and monitoring is enabled to track and alert on all logons and database modifications.	LRS segregation of duties controls adequately manage risk across the Software Development Lifecycle and are in line with industry standards and best practices.
Database Administration practices	LRS PGoldV3 solution utilizes Microsoft's SQL Server as the required database with LACERS data in both a business and audit database that resides on the Team Foundation Server in the LRS Data Center. SQL Server database administrator access is limited to LRS DBAs for customer or departmental database systems that are used by the database administrator, implementation team and product support team as needed for legitimate business need including job requirement.	LRS database administration controls adequately protect the application and sensitive data (in accordance with LRS Information Security, and Privacy Policies), maintain data integrity, and are in line with industry standards and best practices.
Monitoring practices	LRS critical systems are configured to alert their administrator if violations of policy are detected or when user-specified performance or behavioral thresholds are exceeded. LRS monitors and evaluates vulnerabilities on a weekly basis including system components and shared infrastructure for the PGold software, services, servers and all other system components and resources that are included with the PGold solution. The PGold software is also monitored through the threat management gateway and has regular intrusion testing performed by a third-party vendor. Additionally, LRS performs additional monitoring through periodic security assessment by their compliance department.	LRS monitoring controls adequately and continuously confirm information is protected, and security is maintained and are in line with industry standards and best practices.

© 2022 Grant Thornton LLP | All rights reserved

Detailed Assessment – Strengths (cont.)

Assessment Categories	Current Process	Result
Acquisition, development and change-control practices	The PGoldV3 web-based communication uses Secure Sockets Layer (SSL) and certificate-based 256-bit encryption. The security service utilizes Microsoft's Active Directory Lightweight Directory Services (AD LDS) for managing users, user groups, and storing access rights integrated through the security console. Monitoring systems continuously examine and report on performance, availability, and security events or configuration issues. Anti-virus and vulnerability management systems, at both LRS and LACERS, are in place to alerts of potential issues.	Securing application services and protecting transactions include encryption, secure protocols and monitoring are adequate and in line with industry and ISO 27001 standards.
	Within LRS, only employee members of the software development team have access to the server where LACERS data is stored. Access is controlled through an automated ticketing system, appropriate permission is role-based and approved by management. Access to LACERS' application environment is performed as needed by a LACERS administrator.	LRS identity and access management controls adequately manage risk of exposure to LACERS data within the environment and are in line with industry standards and best practices.
Production Control Practices	LRS consistently includes sufficient information on software updates that are performed for PGoldV3. In addition to the information that is included in the PIR notes, LRS provides more detailed information about each PGoldV3 update that is completed and uploads the information to the portal.	LRS production control practices adequately manage communication risk of changes made to the application software for LACERS' version.

© 2022 Grant Thornton LLP | All rights reserved

Grant Thornton

Appendix C

LACERS Stakeholders

© 2022 Grant Thornton LLP | All rights reserved

Workshop Stakeholders

Below are the LACERS stakeholders that participated in the PGoldV3 workshops.

Stakeholders	Role	Date(s) of workshop
Melani Rejuso	Audit Manager	March 2, 17-18; 21; 29-31; April 5
Lauren McCall	Senior Systems Analyst	March 17, 2022
Brian Cha	-	March 17, 2022
Todd Bouey	-	March 21, 2022
Jason Leung	Senior Systems Analyst	March 21, 2022
Cliff Lim	-	March 21, 2022
Thomas Ma	Information Systems Manager II	March 21, 2022
Audrey Dymally	Supervisor, Legal Processing Unit	March 29-30, 2022
Taneda Larios	Member Services	March 29, 2022
Margret Drenk	Senior Benefit Analyst	March 30, 2022
Glen Malabuyoc	Supervisor, Account Reconciliation	March 30, 2022
Lourdes Quintos	Senior Benefits Analyst	March 30, 2022
Maricel Martin	Supervisor, Buybacks	March 30, 2022
Ferralyn Sneed	Chief Benefit Analyst	March 31, 2022
Jamie Roberts	-	March 31, 2022
Susann Hernandez	-	March 31, 2022
Gabriel Bautista	-	March 31, 2022
Christopher Dimano	Counselor, Service Benefits Unit	March 31, 2022
Magda Rodrigues	Manager, Benefits Determination Unit	March 31, 2022
Selina Wong	Supervisor, Payroll	April 5, 2022
Lolette Badar	Accountant, Payroll	April 5, 2022

© 2022 Grant Thornton LLP | All rights reserved

Grant Thornton

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the independent network of GTIL member firms provide services to their clients, as the context requires. GTIL and each of its member firms are not a worldwide partnership and are not liable for one another’s acts or omissions. In the United States, visit grantthornton.com for details.

© 2022 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd