COUNTY AUDIT DEPARTMENT

REPORT # 348

An Audit of:

ORACLE SECURITY ADMINISTRATION

JUNE 14, 2018

Pat Frank INTEGRITY. TRANSPARENCY. ACCOUNTABILITY.

CLERK OF COURT & COMPTROLLER • HILLSBOROUGH COUNTY, FLORIDA

Pat Frank INTEGRITY. TRANSPARENCY. ACCOUNTABILITY.

CLERK OF COURT & COMPTROLLER • HILLSBOROUGH COUNTY, FLORIDA

June 14, 2018

Dear Pat Frank, Clerk of Court and Comptroller:

The Audit Team performed an audit of the Oracle Security Administration control environment (Audit Report # 348, June 14, 2018). Responses to the Audit Team's recommendations were received from the Director of Clerk's IT Enterprise Solutions and Support and have been included in the Report after each audit comment and recommendation.

The purpose of this Report is to furnish management independent, objective analysis, recommendations, counsel, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

The Audit Team appreciates the cooperation and professional courtesies extended to the auditors by the Director and personnel of the Clerk's IT Enterprise Solutions and Support Department during this audit.

Sincerely,

Heidi Pinner, CIA, CISA, CFE, CRMA, Director of County Audit

CC: Dan Klein, Chief of Staff
Rick VanArsdall, Chief Deputy, Clerk to the Board
Tim Simon, Deputy Comptroller
Michelle Decker, Chief Information Officer
Chris Tluczek, Director, Clerk's IT Enterprise Business Solutions

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

In August 2013, Hillsborough County went live with the Oracle E-Business Suite (EBS) enterprise resource planning system known as Oracle EBS. The Oracle EBS system centralizes various functions and data related to accounting, procurement, human resources, fixed assets, reporting, suppliers, capital projects, grants, and other areas of the organization. Oracle EBS is a multi-agency shared-tenancy agreement (shared between the Clerk, the County and the City of Tampa) and hosted by a third-party on-demand service.

Oracle EBS system users are granted access to specific Responsibilities that allow them to access and perform certain tasks based on the employee's job duties. A number of Oracle users have access to sensitive areas such as approving payments, setting up new vendors, posting journal entries, or accessing personal information. Deciding which Responsibilities will be granted to particular users and what changes are made to the components of those Responsibilities (change management) are key aspects of the Oracle security administration process.

The Clerk's IT Enterprise Solutions and Support Department (ESS) is responsible for the Oracle EBS security administration activity for all users of the Board of County Commissioners (BOCC), the Clerk of Circuit Court (Clerk) and other independent agencies such as Civil Service, Environmental Protection, Court Administrator (13th Judicial Circuit), Supervisor of Elections and Planning Commission.

OBJECTIVE

The objective of the audit was to determine whether or not the Oracle Security Administration control environment provides a reasonable level of assurance that users and system security procedures are appropriately controlled, documented, and monitored. This audit also serves as a follow-up on open recommendations from Audit Report # 282, *Oracle E-Business Suite Security Administration Activity,* issued May 4, 2015.

SCOPE

The audit was conducted in conformance with the *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The audit scope focused on the Oracle security administration control activities over users under the Clerk of Court and BOCC as of January 18, 2018.

OVERALL EVALUATION

The employees of ESS were responsive to the Audit Team's inquiries and politely provided the information as requested. The Audit Team encountered knowledgeable and dedicated employees during the course of the audit.

The following table summarizes the audit comments and corresponding cross references to the page number where the audit comment details can be found in this Report.

AUDIT COMMENT	CONCLUSION OF OBJECTIVE	PAGE
1	Opportunities exist to improve the internal controls surrounding the Oracle Security Administration function.	3
2	Oracle user access Responsibilities were properly approved and set up in the system.	7
3	There is an opportunity to improve the procedures to record change management approvals.	9

OPINION

The overall control environment relative to the Oracle EBS security administration function is at a formal (defined) maturity level. Management has controls established and documented with a policy structure which reasonably ensures that the Oracle security administration process is carried out in an appropriate manner and that control gaps are detected and remediated in a timely fashion. Some exceptions were noted and opportunities were identified to strengthen the controls related to the change management process and monitoring capabilities. Addressing these opportunities will enhance the overall control structure and provide increased consistency and assurance.

The exit conference was held on May 16, 2018.

Other minor concerns not included in this Report were communicated to management and/or corrected during fieldwork.

AUDITED BY

Heidi Pinner, CIA, CISA, CFE, CRMA, Director of County Audit
Ben Everett, CPA, CIA, CFE, Audit Manager
Raul Cardona, CIA, CISA, CAMS, Senior Internal Auditor

AUDIT COMMENTS & RECOMMENDATIONS

AUDIT COMMENT 1

Opportunities exist to improve the internal controls surrounding the Oracle Security Administration function.

The objective was to determine whether or not there are appropriate controls over the Oracle Security Administration function and to determine if related risks have been effectively mitigated.

Using a control framework developed by the Information Systems Audit and Control Association (ISACA), the Audit Team conducted interviews with Clerk’s IT management and staff to assess the Oracle EBS System Security control environment. The Audit Team also reviewed documentation associated with these controls and performed testing to determine whether or not:

1. Security administration and change management policies and procedures were in place, properly formalized and documented.

2. There was an organizational structure for the security administration function in place.

3. Responsibilities related to information security administration were defined and assigned.

4. Alerts and monitoring reports have been used to monitor security events, as well as being generated and reviewed on a regular basis.

5. Account default passwords have been changed.

6. Security password configuration standards have been developed and enforced.

7. Users had a unique user identifier within the Oracle application.

8. Monitoring activities are being performed to ensure that access privileges are reviewed and sensitive data is restricted to authorized users only.

9. Logs for unauthorized access attempts are monitored, recorded and reviewed.

10. A process is in place to ensure that Responsibilities are assigned with an appropriate Segregation of Duties (SOD).

11. Test and production environments are segregated and protected by logical access controls.

TESTING RESULTS

Through inquiries, observations and testing, the Audit Team determined that:

1. Oracle EBS security policies and procedures are established. However, the Oracle Security Administration procedure has not been formally updated since 2013.

2. An organizational structure is in place for the Clerk's Oracle Security Administration activity with defined roles, responsibilities and levels of authorization. However, a formal policy and structure is not in place to govern the multi-agency relationship for the Oracle instance.

3. The Oracle Security Administrator responsibility appears adequately defined and is assigned solely to members of the Clerk's security support team.

4. Security alerts have been established for new employee hires and terminations. However, this is a passive control that alerts a user to take action without a mechanism to ensure the appropriate action was executed. This leaves the process subject to errors and omissions.

5. Default manufacturer account passwords for Oracle EBS had been changed in the Production instance.

6. Password and access settings had been configured to;

   a. Ensure password complexity and length (Strong passwords with an 8 character minimum)
   b. Enforce access failure limits
   c. Enforce password expirations
   d. Prevent password recycling, and
   e. Time out user sessions when inactive.

   The above password configurations meet minimum recommendations for password security.

7. Each employee has a unique, sequentially assigned user identifier required to log into the Oracle application.

8. Clerk's Oracle Security Administration has a process in place to perform user access reviews annually. This review includes a request to the management of each user department to review and certify that all existing users have appropriate levels of system access. This process is dependent on the participation of department management and does not include temporary/generic accounts.

9. Logs for unauthorized access attempts are being generated. However, logs are currently not being reviewed or analyzed.

10. The process of assigning Oracle Responsibilities includes SOD controls. However, automated SOD monitoring has not been implemented.

11. The test and production environments are properly segregated and each environment has respective access controls in place.

RECOMMENDATION

Management should consider enhancing the Oracle EBS Security control environment by:

- Updating the Oracle EBS Security Administration policy and establishing a periodic review interval to ensure future changes are adopted and approved by management timely.

- Establishing, in conjunction with the other participating agencies, a formal and defined governance policy structure for the Oracle instance.

- Determining if enhanced controls can be implemented to reduce the risk of error or omission in the user hire and termination process.

- Including requirements for the periodic user access reviews as part of the multi-agency governance policy when implemented.

- Ensuring that user access reviews include the review of all active Oracle temporary/generic accounts and disabling any accounts that are no longer needed.

- Implementing an advanced data analytics tool to improve the security and continuous monitoring capabilities of the Oracle EBS system by:

    - Enhancing monitoring alerts for changes/updates into production servers.
    - Better monitoring of user access privileges and sensitive data being accessed.
    - Improving analysis and examination of unauthorized access attempt logs.
    - Implementing an advanced segregation of duties monitoring capability to identify incompatible privileges, Responsibilities and user functions.

CLIENT RESPONSE:

- *Concur*

CORRECTIVE ACTION PLANS:

1. *Enterprise Solutions and Support (ESS) Management will create a yearly procedural process to review and update the Oracle EBS Security Administration Policy on an ongoing basis.*

2. *Clerk Senior Management (Tim Simon and Rick VanArsdall) will meet with other Senior Management from BOCC and City. The members of the Governance team will work towards building a Memo of Understanding (MOU) for Post Go live Support for ERP.*

3. *ESS will review current new hire/terminations processes. The goal will be to include automated alert notifications from Oracle into the new Clerk Manage Engine – Ticket system with automatic workflows.*

4. *ESS will continue to perform Annual Security reviews including the review of user, temporary/generic accounts and disable when no longer required.*

5. *ESS and County Finance will work with Appssurance Vendor on the implementation of Oracle Governance Risk and Compliance (GRC) modules Advance Controls Governance (ACG), Change Controls Governance (CCG) and Transactions Control Governance (TCG).*

TARGET COMPLETION DATES:

1. *7/30/18*

2. *3/30/19*

3. *9/30/18*

4. *8/30/18*

5. *12/30/18*

AUDIT COMMENT 2

Oracle user access Responsibilities were properly approved and set up in the system.

The objective was to determine whether or not there are adequate controls in place to ensure that Oracle user account provisioning is accurately performed and system access is properly approved.

The Audit Team reviewed the user provisioning process, selected a random sample of 50 Oracle user accounts and performed the following audit procedures:

- Reviewed every Oracle responsibility assigned for each of the user accounts in the sample.

- For every user account with a financial or managerial Oracle responsibility, the Audit Team reviewed the respective Oracle Security form to ensure that the form was appropriately completed and that approval was properly obtained.

- In addition, for every user account in the sample with a financial Oracle responsibility assigned, the Audit Team verified that a signed "Confidentiality Form" was completed as required by the policy.

TESTING RESULTS

Twenty-two (22) out of 50 users (44%) in the sample had the default (minimum) Oracle Responsibilities assigned to them. No Oracle Security or Confidentiality form is required for these users. The remaining 28 out of 50 users (56%) had financial Oracle Responsibilities assigned to them and required an Oracle Security form or management email approval.

- Twenty-seven (27) out of the 28 (96%) users with financial Oracle Responsibilities assigned had the proper supporting documentation with management approval. The Oracle Security form for one user out of 28 (4%) was not signed by the employee's supervisor/department director.

- Twenty-seven (27) out of 28 (96%) users with financial Oracle Responsibilities had a Confidentiality Form on file. One user out of 28 (4%) was noted as not having the Confidentiality Form on file as required by the policy.

A quality assurance process is in place to monitor user access changes. This process currently confirms that each properly documented request has been appropriately executed. However, the process does not take into account whether an unintended or undocumented change occurred.

RECOMMENDATION

No significant exceptions were identified for the Oracle user account provisioning process. To further enhance this process, management should:

- Ensure that all required approvals and forms are obtained prior to granting user Responsibilities access and that the forms are appropriately maintained.

- Develop a mechanism to prevent or detect unintended or undocumented user changes.

CLIENT RESPONSE:

- *Concur*

CORRECTIVE ACTION PLANS:

1. *ESS will continue to improve the process of Oracle Security Request utilizing the OnBase Unity E-forms and workflow process and Clerk ticket system Manage Engine.*

2. *ESS will review Oracle GRC CCG module and utilize log reports to monitor provisioning of Oracle Responsibilities.*

TARGET COMPLETION DATES:

1. *3/30/19*

2. *12/31/18*

AUDIT COMMENT 3

There is an opportunity to improve the procedures to record change management approvals.

The objective was to determine whether or not there are adequate controls in place over the change management process for Oracle Responsibilities.

As part of the change management controls, an Excel document called "TC200 form" is created for every Oracle application managed by Clerk's IT. This form serves two main purposes. First, it lists all the Responsibility functions, menus and security rules (or exclusions) related to the Oracle application. Secondly, anytime a change is made to a menu, function or exclusion of the application, the TC200 form is updated to keep track and maintain a record of the change performed.

Absent an advanced analytic tool, Administrators do not currently have the ability to detect un-documented changes to the Oracle system.

To test the existing process, the Audit Team performed the following audit procedures:

- Located the TC200 form for each of the 15 applications supported by ESS to ensure that the form was properly maintained.

- Selected a random sample of 20 changes from the list of TC200 forms for testing.

- For each of the 20 changes in the sample, the Audit Team pulled the following supporting documentation from Clerk's IT SharePoint for testing:

  - SharePoint Ticket
  - EBS Change Request Form
  - Testing supporting documentation (when applicable)
  - Different applicable levels of approval based on the type of change: Business, Functional, Technical, Governance and/or City (Oracle EBS is a shared joint system also used by the City of Tampa).

- Selected a judgmental sample of ten (10) Oracle Responsibilities from the applications managed by ESS.

- Obtained the Function Security Menu Report (FSMR) for each responsibility in the sample showing all the functions, menus and security rules/exclusions that restrict access to specific user responsibility functions.

- Compared the FSMR for each Oracle responsibility in the sample to the respective TC200 form to ensure that every security rule/exclusion included in the TC200 was properly listed in the FSMR and vice versa.

TESTING RESULTS

Based on the audit tests performed:

- Thirteen (13) of 15 (87%) TC200 forms were properly maintained in the SharePoint site. The remaining 2 TC200 forms (Learning Management and Performance Management for Human Resources applications) were not developed as of the time of audit testing, March 2018.

- All of the changes selected in the sample had a ticket created and maintained in the SharePoint system.

- Fifteen (15) of the 20 changes selected in the sample required a Change Request Form. All 15 changes had one on file.

- All changes requiring testing to be performed prior to moving changes into production had applicable testing supporting documentation.

- Depending on the type of change, each change could require up to 5 different approvals (Business, Functional, Technical, Governance and City). For the sample of 20 changes selected, there were a total of 60 approvals required.

- Fifty-four (54) of the 60 required approvals (90%) were properly documented. The remaining 6 approvals (10%), pertaining to 4 change requests, could not be found.

- One change request out of 20 (5%) has been on an open ("pending") status for Governance approval since January 2015 and it remains unimplemented.

- All Oracle application Responsibilities selected for testing had matching security rules/exclusions between the TC200 form and the respective FSMR.

RECOMMENDATION

Management should consider enhancing the controls over the change management process by:

- Making sure a TC200 form is created and maintained for each Oracle application.

- Making certain that all change approvals are properly obtained and clearly documented in the change request form or the SharePoint ticket.

- Implementing an advanced data analytics tool to monitor for application configuration changes.

CLIENT RESPONSE

- *Concur*

CORRECTIVE ACTION PLANS:

1. *ESS will create and maintain TC200 forms for each Oracle application.*

2. *ESS will utilize the Clerk ticket system Manage Engine and its workflow to review Oracle changes and ensure all proper documentation and approvals are obtained.*

3. *ESS and County Finance will work with Appssurance Vendor on the implementation of Oracle Governance Risk and Compliance (GRC). Specifically the module Change Controls Governance (CCG).*

TARGET COMPLETION DATES:

1. *9/30/18*

2. *12/30/18*