PAT FRANK
Clerk of the Circuit Court
13th Judicial Circuit

COUNTY AUDIT

HILLSBOROUGH COUNTY, FLORIDA

ORACLE E-BUSINESS SUITE SECURITY ADMINISTRATION ACTIVITY

REPORT # 282

MAY 4, 2015

PAT FRANK
Clerk of the Circuit Court
13th Judicial Circuit

May 4, 2015

Dear Pat Frank, Clerk of the Circuit Court:

The Audit Team performed an audit of the Oracle E-Business Suite (EBS) security administration activity (Audit Report # 282, dated May 4, 2015). Responses to the Audit Team's recommendations were received from the Systems Support Director and have been included in the Report after the audit comment and recommendations.

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 Systems Support during this audit.

Sincerely,

Peggy Caskey, CIA, CISA, CFE
Director of County Audit

CC: Dan Klein, Chief of Staff
Rick VanArsdall, Chief Deputy, Finance
Mary Strommer, Systems Support Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

In August 2013, the Oracle E-Business Suite (EBS) enterprise resource planning system went live. Systems Support conducts the Oracle EBS security administration activity for all Board of County Commissioners (BOCC) and Clerk of Circuit Court (Clerk) users. The security administration activity includes the provisioning of user access, approval rights, and workflow within the Oracle EBS modules. The City of Tampa has a separate security administration activity, which serves in this capacity for the City's users.

OBJECTIVE

The objective of the audit was to determine whether or not the control environment of Systems Support's security administration activity provides a reasonable level of assurance that user and system security is appropriately controlled, documented, and monitored.

SCOPE

The audit was conducted in accordance 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 Team evaluated Systems Support's security administration activity control environment as of November 2014. This evaluation included:

- Discussions with Systems Support personnel responsible for the security administration activity and completion of an internal control questionnaire.
- Collection and review of supporting documentation to confirm control implementation.
- Sample testing key control components including user provisioning and privileged user access.

OVERALL EVALUATION

Systems Support's personnel were responsive to the Audit Team's inquires and provided data and other requested information in a prompt and courteous manner. The Audit Team found Systems Support's personnel to be knowledgeable and dedicated employees who were receptive to the Audit Team's suggestions for improvements.

AUDIT COMMENT	CONCLUSION OF OBJECTIVE	PAGE
1	Opportunities exist to enhance Systems Support's Oracle EBS security administration controls.	3

OPINION

The security administration activity control environment is at the repeatable maturity level. Controls have been established with some policy structure, but formal process documentation is still needed and process consistency has not yet been attained. Implementing the recommendations in the Report will help the security administration activity reach the next maturity level.

The exit conference was held on March 6, 2015.

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

AUDITED BY

Peggy Caskey, CIA, CISA, CFE, Director of County Audit
Mary Ann Kominsky, CIA, CISA, CPA, IT Audit Manager
Heidi Pinner, CIA, CFE, Senior Auditor

AUDIT COMMENT & RECOMMENDATIONS

AUDIT COMMENT 1

Opportunities exist to enhance Systems Support's Oracle EBS security administration controls.

The Audit Team determined whether or not the control environment of Systems Support's security administration activity provides a reasonable level of assurance that user and system security is appropriately controlled, documented, and monitored.

The Audit Team worked with Systems Support personnel to complete a security administration internal control questionnaire and to gather supporting documentation and evidence of existing controls. The Audit Team performed sample testing on key control components.

Test results indicate that Systems Support implemented several controls that help mitigate the risks associated with the security administration function.

- A change management procedure with appropriate approval requirements has been defined, implemented, and communicated for user and system security changes.
- A log of requested and executed changes is maintained.
- An organizational structure has been defined. Security administration functions and responsibilities related to information security have been segregated, defined, and assigned.
- Password controls, unique user IDs, and a session time out interval are in place to restrict access to programs, data, and other information resources.
- All successful and unsuccessful access attempts are logged.
- Common default user IDs and passwords are not utilized.
- Ability to execute reports is limited by assignment of responsibilities. Reports and query outputs are restricted to the requesting user.
- Active user IDs, responsibilities, and approval authorizations are documented and refreshed weekly.
- An initial user security confirmation has been performed and is scheduled to be conducted annually.

There are opportunities for Systems Support's security administration activity to enhance the control environment.

1. Formal governance polices/procedures have not been fully developed or implemented for the security administration activities within the Oracle EBS system.
2. Routine monitoring procedures have not been developed for all necessary areas of the security administration function.
3. Advanced analytics/monitoring tools are not yet implemented or available for key security administration functions. Periodic monitoring is not performed on master data changes.
4. The existing change management process is manual and, therefore, susceptible to user error or omission.
5. User access change management procedures have been formalized and documented but test results indicate some inconsistency in the application of these controls.

   Oracle user access requests are maintained in the OnBase document management system once completed. The Audit Team identified 83 requests to delete, inactivate, or create user access or approval rights as of November 24, 2014, and judgmentally selected 27 of these requests for testing. There were 179 modification requests that were also identified but were not evaluated as part of this review. Initial user set up was part of Oracle EBS implementation. These initial set ups were confirmed by Systems Support via the previously mentioned user security and approval confirmations.

   Of the 27 requests tested:

   - 82% of the requests had evidence of the appropriate departmental approval prior to execution of the request. The remaining 18% either were missing this approval or obtained the approval after the request was granted.
   - 85% of the requests had evidence of the Systems Support Director’s approval prior to execution of the request. The remaining 15% either were missing this approval or obtained the approval after the request was granted.
   - 100% of the 27 requests indicated when the request was completed and by whom.

- 74% of the requests had a quality assurance review; however, 10% of the reviews occurred 40+ days after the execution of the request. The remaining 26% of the requests did not have a quality assurance review performed.
- 100% of the 27 requests had system access that was consistent with the request(s) on file.

6. Unused, default responsibilities have not been end dated in the system and remain available for assignment.
7. The responsibility titled Application Administrator is used for user security set-up. Application Administrator is assigned to users outside of the security administration team.

RECOMMENDATION

1. Consideration should be given to defining a formal governance policy and procedure for security administration activities within Oracle EBS.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

The joint implementation (Project 1) of the new ERP system by the BOCC, City of Tampa and Clerk of Court introduced all three agencies to not only dramatically more complex functionality, but the increased complexity of operating in a multiagency, shared-tenancy software application hosted externally by a third-party on-demand service. This new system required adopting a new paradigm for supporting and managing application security that was not needed in traditional IT environments. Risks associated with any technology environment including controlling access, enforcement of business rules and data security are complicated by the multitenant environment that includes shared data files, common security administration, a single supplier and customer master file and a shared data warehouse application (OBIEE). Unlike in the former legacy world of single tenant applications where physical separation of data (air gaps) simplified the design of application and data security, multitenant application environments rely almost exclusively on *application configuration and security settings to control the integrity and access to data and functionality between application tenants.*

For the Project 1 implementation, a formal project governance structure is in place. It includes senior management from the County, City of Tampa, Civil Service Board, and Clerk of Court providing oversight of the project. Each of the agencies provided required project management services related to their portion of the project. However, since the initial go live of the Oracle EBS financial applications in August 2013, the Clerk of Court ERP System Support department has assumed responsibility for the ongoing support and administration of system wide security and change control as well as functional and technical support of financial and payroll applications. The City of Tampa performs its own security and application administration in the shared environment for their employees.

In the absence of a formal joint agency operating governance structure, ERP System Support has operated under guidance and oversight of the Clerk's management structure and worked to keep the other agencies and Project 1 governance apprised of its practices and procedures.

On behalf of the BOCC and Clerk organizations, the ERP System Support has adopted processes and procedures similar to those it employed for its legacy applications. To meet the more stringent demands of the multitenant environment, the department also looked to best practice recommendations from organizations like the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), industry experts like SANS and Gartner and Oracle's application security recommendations to establish security management practices for EBS. ERP System Support also coordinated with the EBS support team at the City of Tampa on security administration activities.

With the closeout of Project 1 activities imminent, senior management for the BOCC, City of Tampa and the Clerk of Court are working to define and establish an ongoing governance structure for shared ERP applications including Oracle EBS, OBIEE, Kronos, Hyperion and Tele-staff as well as the third-part hosting service. Once established, a principal role of governance will be to adopt *uniform policies and practices for all aspects of controlling the health and security of the ERP environment.*

This process and it's time schedule is not under the control of the ERP System Support department or of the Clerk of Court alone.

As Project 1 is being closed out, senior management for the BOCC, City of Tampa, and Clerk of Court are working on defining an ongoing governance structure for the ERP Environment. ERP System Support recommends reviewing this issue in six months (9/30/2015).

TARGET COMPLETION DATE

9/30/2015

RECOMMENDATION

2. Consideration should be given to developing routine monitoring procedures and intervals for key system and security administration processes.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

While the ERP System Support department fully agrees with the recommendation, nearly all available resources have been fully engaged in stabilizing the new Oracle EBS application and developing processes to meet the day-to-day operating demands of the system. Select processes like security confirmations are in place, but even these will require additional work to make them more effective and efficient. Other process such as regularly scheduled reviews of inactive or stale user accounts, periodic analysis of the unsuccessful logon report, reviews of support team users with exceptional privileges, and periodic review and testing of security configurations and provisioning have not been implemented.

The extent to which these practices can be fully implemented will depend on the availability of support resources to implement and carry them out. Until formal governance structure is in place that can weigh the cost of providing full *security management versus the risk of not doing so is in place, progress will be made as time and resources allow by the current ERP System Support team.*

ERP System Support recommends reviewing this issue in six months (9/30/2015) to allow for formalization of a multiagency governance structure and its impact on the availability of support resources and governance standards.

TARGET COMPLETION DATE

9/30/2015

RECOMMENDATION

3. Consideration should be given to implementing advanced analytics and monitoring tools to aid in the review of key processes including master data changes, privileged user access, and segregation of duties.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

As discussed above in the response to Recommendation 1, security administration for the Oracle E-Business Suite is complex for several reasons, but foremost is the overall complexity of the application's integrated functionality as well as the additional complexity introduced by the multiple agency shared-tenant environment.

For the County (BOCC and Clerk) there are more than 6,000 active users in EBS. There are 240 assigned responsibilities which total more than 29,000 security configurations. In addition to security records, there are more than 23,000 workflow approval configurations active in EBS.

The Clerk recognized that managing the risk associated with such a complex security environment required an automated set of tools to help enforce the integrity of the EBS environment.

In July 2014, the Clerk approved a project to license and implement the Oracle Governance, Risk and Compliance (GRC) Application Suite. When operational, Oracle GRC will provide a set of tools that will assist the Clerk with automating current manual processes and provide administrators with a better understanding of the status of compliance activities and manage compliance in a disciplined fashion.

The implementation of the Oracle Governance, Risk and Compliance (GRC) application is in process. An estimated completion date is scheduled for September 30, 2015.

TARGET COMPLETION DATE

9/30/2015

RECOMMENDATION

4. Consideration should be given to automating the existing change management process and logging procedures.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

The Clerk of Court has approved a project to implement a new support management system using the Clerk's existing OnBase application. This system will be developed on a phased basis and will eventually replace both an outdated HP Service Desk (SM7) application used for supporting the Clerk's OnBase and internal systems and the SharePoint based tracking system used to support the Oracle EBS Financial applications. The new application will also fully support automation of the change management process including required approvals.

TARGET COMPLETION DATE

06/30/2016

RECOMMENDATION

5. Consideration should be given to implementing controls or monitoring activities to ensure that security request forms and user access changes are requested, applied, reviewed and maintained consistently.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ERP System Support is in the process of updating all security request forms to include better workflow tracking included QA reviews. Together with updating security administration procedures the issues identified in the security review should be resolved. In addition, as the Project 1 implementation process winds down and the system continues to be stabilized, security administration resources are able to focus more time and attention toward maturing its processes.

TARGET COMPLETION DATE

07/31/2015

RECOMMENDATION

6. Consideration should be given to end dating the unused responsibilities within the Oracle EBS system so that they are not erroneously assigned to an active user account.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ERP System Support is in the process of reviewing all available EBS responsibilities to determine those that should be end dated.

There are currently 2,239 responsibilities in the EBS Application. 1750 of these are currently available for assignment. Of these, 1341 responsibilities that have never been used and 23 are inactive. These 1364 are currently being considered for end dating. ERP System Support will coordinate this activity with the City of Tampa and BOCC support teams.

The following tables summarize the current responsibility statuses.

All EBS Responsibilities	***Number***
End Dated Responsibilities Never Used	*486*
End Dated Responsibilities Inactive	*3*
Available Responsibilities	*1750*
Total Responsibilities in EBS	***2239***

Available Responsibilities	***Number***
Available Responsibilities in Use	*386*
Available Responsibilities Inactive	*23*
Available Responsibilities Never Used	*1341*
Total Available Responsibilities	***1750***

TARGET COMPLETION DATE

05/29/2015

RECOMMENDATION

7. Consideration should be given to further limiting the access to the responsibility titled Application Administrator to only appropriate members of the security administration team.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

On 03/06/2015 ERP Support Issue No 2563 was created to replace the Application Administrator into two separate administrator responsibilities. One will contain only security and workflow configuration functionality and the other *will include all other administration functionality required for production support except for security. After the new responsibilities have been created, Application Administrator will be end dated and no longer available for day-to-day use in either production or non-production instances.*

TARGET COMPLETION DATE

06/30/2015