

Internal Audit Report on Database Administration Oracle Enterprise

County of Henrico



*Proud of our progress;
Excited about our future*

**Internal Audit Report #247
August 5, 2015**

HENRICO COUNTY INTERNAL AUDIT
<http://henrico.us/audit>
4301 EAST PARHAM ROAD
P.O. BOX 90775, HENRICO, VIRGINIA 23273-0775

Internal Audit Report on Database Administration – Enterprise



Report #247
August 5, 2015

1



Audit Summary

- Scheduled Audit
- Conclusions on Audit Objectives
 - ◆ Determine that database policies, configuration settings, hardening procedures and patch processes are in place and appropriate.
 - ▲◆ Determine that access, user accounts, database permissions and password controls are sufficient and effective.
 - ▲ Determine that restoration and backup procedures are sufficient and effective.
 - Determine that database auditing and monitoring activities are sufficient and effective.
- Exception Oriented
- 2 reportable Issues and 1 Other Observation
- Management Action Plans have been developed to address all risks identified.

■ Sufficient ▲ Needs Improvement ◆ Insufficient – Needs Immediate Attention ◆ Risk previously identified-Action Plan in Progress

County of Henrico Internal Audit

2



Contents

- Introduction and Background
- Scope, Internal Controls, and Methodology
- Conclusions on Audit Objectives
- Issues and Management Action Plans
- Closing and Report Distribution



County of Henrico Internal Audit

3



Introduction

- IT Auditor III, Sharon Thornton, performed audit work
- Used professional auditing standards
- Examined controls & tested for selective compliance
- All exceptions given to Agency
- Reported control design issues & significant test exceptions only
- Work for same Government we audit



County of Henrico Internal Audit

4

Background

There are 2 database administrators that support Oracle Enterprise databases.

There has been a trend of moving away from Oracle Enterprise databases.

- This is impacted by what databases the application vendors support and the platform they use for development.
- Analysis of department needs, performance, cost, and available hardware/software determines the appropriate database to be selected.
- Additionally, a system using a Linux operating system requires an Oracle database.

Oracle Enterprise licenses are perpetual which means the same license can be used for multiple versions. The current licenses were purchase over 15 years ago.

5



Background: Oracle Enterprise Database Administrators' Goals

- Keep databases secure
- Keep databases running efficiently
- Keep databases available 24X7

Source: Information Technology Project Leader



Background: Oracle Enterprise Databases Supported

Database Versions	Number of Databases
[Redacted]	

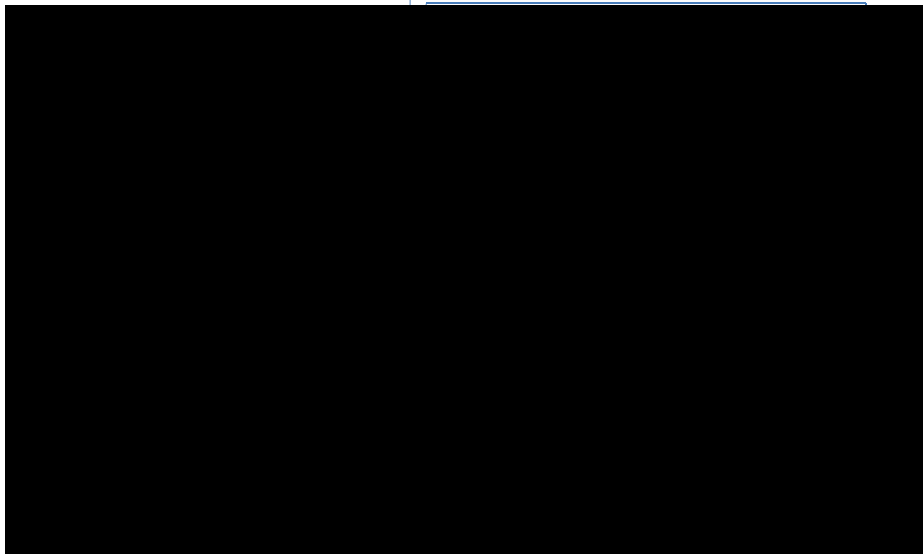
Some of the Applications whose data is maintained in Oracle Enterprise databases are:

[Redacted]



Background: Oracle Architecture

Client Process





Audit Scope

In-Scope:

- Information Technology
 - Database administrators
 - Selected system administrators
- Selected Oracle Enterprise databases
- Selected operating systems



Out-Scope:

- Oracle databases that hold [REDACTED] data (general ledger and human resources)
- All other agencies and departments (including Schools)
- All other County application, database, and operating systems



Internal Controls

Objectives

- Reliability and integrity of information
- Compliance with policies, procedures, laws and regulations
- Safeguarding of assets
- Effectiveness and efficiency of operations





Internal Controls Cont'd

General Limitations of any Controls

- Errors and irregularities may go undetected
- Inherent limitations in any control structure including:
 - resource constraints
 - legislative restrictions, etc.
- Projection to future subject to risk of change in effectiveness
- Compliance may deteriorate



Audit Methodology

1. Evaluated internal control systems through completion of questionnaires
2. Validated answers to questionnaires by sample testing and securing evidence
3. Performed walkthroughs to obtain an understanding of the database administration processes
4. Evaluated policies and procedures and sample tested for compliance





Conclusions on Audit Objectives

Objective	Conclusion
A. Determine that database policies, configuration settings, hardening procedures and patch processes are in place and appropriate.	**
B. Determine that access, user accounts, database permissions and password controls are sufficient and effective.	** (Issue 1 and Other Observation 1)
C. Determine that restoration and backup procedures are sufficient and effective.	 (Issue 2)
D. Determine that database auditing and monitoring activities are sufficient and effective.	

** Based on Network Vulnerability Assessments in FY13 & FY15, management was previously made aware of existing configuration management issues partially caused by Information Technology's limited involvement in some acquisitions of vendor systems. No new configuration management issue is being noted here as management action plans are already pending completion to address those issues.

Sufficient Needs Improvement Insufficient – Needs Immediate Attention Risk previously identified-Action Plan in Progress
County of Henrico Internal Audit 13



Issues

1. Implement User Password Security in Community Development System
2. Ensure Offsite Backup Frequency and Retentions Meet Business Needs

Other Observation

1. Set Password Profile Values to Recommended Settings



Implement User Password Security in Community Development System



Condition

██████████, the County's central Community Development application, has one of two Oracle databases purchased by the County where the application users are authenticated through the database instead of the application.

Application users are not required to change their passwords as this would require them to directly enter the database to make the changes, which is not desirable. Only the system administrators are required to change their own passwords.

Within the application there is a password change button that is not operational.

There are plans to replace the ██████████ and requirements are currently being written for the RFP. One of the requested features will be integration with Active Directory which will eliminate the existing password problems.



Effect

Without periodic password expiration, if an individual who is able to reach the [REDACTED] login screen learns another user's ID and password, they could use that information to gain inappropriate access to the system indefinitely.

There are risks that this may not be resolved in the system replacement process as not all requirements in an RFP are generally obtainable when discussions begin with the various vendors.

Cause

[REDACTED] is an old system that does not have certain password security controls that are common for the number of system users. The software has been acquired by another company, [REDACTED], that no longer has technical staff familiar with the system.



Criteria

ISACA's Cobit 5 DSS05.04 Manage User Identity and Logical Access states "Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes".

It goes on to state, "authenticate all access to information assets based on their security classification, co-coordinating with business units that manage authentication with applications used in business processes to ensure that authentication controls have been properly administered".



Recommendation

Ensure the planned [REDACTED] replacement will support user security and the ability for users to change their own passwords in the application should the desired link to Active Directory not be feasible. Include such requirements in the RFP and supplier negotiations.

Unless an interim solution is developed while the County continues to use [REDACTED], management will be accepting the risk related to the lack of changing passwords and will be relying on any mitigating controls in the related business processes until a new system is implemented.



Management Action Plan

1. There is an open service case with [REDACTED] regarding the non-working "Change Password" feature in [REDACTED]. IT will continue to follow on this request.

By Whom: Information Tech Project Leader (Community Development Services)

Expected Completion: 1/28/2016

2. The Project Management Team assigned to replace the Tidemark System will ensure the new system meets or exceeds the requested user security configuration.

By Whom: Information Tech Project Leader (Community Development Services)

Expected Completion: 9/30/2016



Ensure Offsite Backup Frequency and Retentions Meet Business Needs



Condition

Based on the four databases sampled, the offsite backups (full server backups that include the databases) are performed weekly.

The backups are:

- sent offsite at the end of the week and
- returned to the County data center the following week where they will be kept two additional weeks.

This means that if a disaster occurred which destroyed the data center and servers located there on Thursday, for example, there could be up to four days of transactions that would be lost if the County relied on the offsite backup to recover.



Effect

Insufficient offsite backups could create significant data loss in the event of a disaster destroying the data center and the servers located there.

Cause

Employees responsible for backups retired and the team currently responsible is in the process of catching up. This team is also in the process of upgrading the backup tools, policies, and procedures with an expected completion by the end of July 2015.



Criteria

ISACA Cobit 4.1 DS4.9 Off-site Backup Storage states,

- Store off-site all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans.
- Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the off-site storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security.
- Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.



Recommendation

While in the process of developing new policies and procedures, survey agencies concerning the frequency and retention of offsite server backups (including databases) and ensure offsite rotation is appropriate to meet their business needs in the event of disaster.



Management Action Plan

We will have additional backup capabilities in the next 30-45 days to do additional monthly backups to tape (located here at [REDACTED]) with longer off-site retention capabilities (>90 days), if required, to Iron Mountain. We also have plans to place our tertiary [REDACTED] array (C3) off-site at either an alternative Henrico County location or commercial co-location facility within the next 90-120 days. This will then give us backup data spread out over three disparate locations and should alleviate any concerns about data recoverability.

By Whom: Information Tech Project Leader (System Administration)
Expected Completion: 12/31/2015



Other Observation

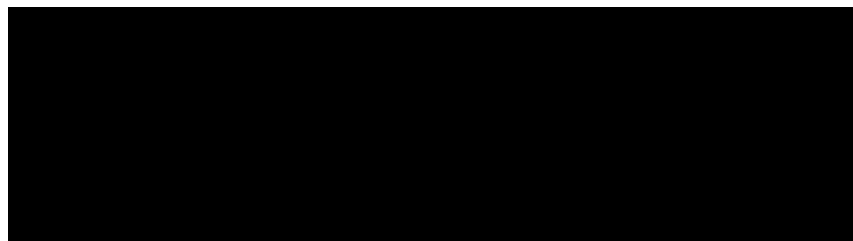
The following slides include an observation noted during our review which was not considered critical in reaching our conclusions on our audit objectives.



Other Observation 1

Set Password Profile Values to Recommended Settings

The Henrico County Password Policy does not define Oracle Enterprise database password profile settings. Password profiles in the databases are not tied to this policy except for complexity. Below are the current password profiles settings for the sample databases:





ISACA's Security, Audit and Control Features Oracle Database 3rd Edition, recommends the following settings:

Failed Login Attempts: 5
Password Life Time: 90
Password Grace Time: 3
Password Lock Time: 1
Password Reuse Time: 90



Recommendation

Adjust profile parameters for passwords to recommended settings or stronger settings (i.e., Password Reuse Time 365 days).



Management Action Plan

We have set the values to those suggested in the ISACA book. However, the Password Limits Lifetime was set to Unlimited in the [REDACTED], [REDACTED] and [REDACTED] as the databases only have Service accounts. [REDACTED] Password Limits Lifetime are set to Unlimited or 180 days as approved by a former IT Project Manager.

By Whom: Information Tech Project Leader (DBA)
Expected Completion: 7/2015 (Completed)



Closing

- Appreciate Agency's cooperation
- Follow up on open Action Plans will be performed as completion dates are reached or after sufficient time has passed to ensure the actions are effective and on-going





Report Distribution

Audit Committee (Mr. Glover, Mrs. O'Bannon, County Manager)	Board of Supervisors, Non-Committee Members
Deputy County Manager for Administration	Director of Information Technology
Internal Audit Staff	



Audit Contact Information

Sharon Thornton, IT Auditor III

Phone: 804-501-7379

E-mail: tho89@henrico.us

Vaughan Crawley, Director of Internal Audit

Phone: 804-501-4292

E-mail: cra85@henrico.us