Audit Review of Database Administration and Controls

Project Number: IM.DATADMN.2013
# Audit Review of Database Administration and Controls

## Table of Contents

- Project Completion Letter .............................................................................................................. 2
- Function Responsibility and Internal Control Assessment.......................................................... 3
- Executive Summary of Observations, Recommendations and Management Responses ....... 4
- Background .................................................................................................................................... 9
- Objective ......................................................................................................................................... 9
- Scope .............................................................................................................................................. 9
- Methodology ................................................................................................................................... 9
- Observations and Recommendations ........................................................................................ 11
- Database Policy and Procedures ................................................................................................ 11
- Conclusion .................................................................................................................................... 13
- APPENDIX A – NeighborWorks Databases ................................................................................. 14
- APPENDIX B – Suggested Stored Procedures for IM Review ..................................................... 15
- APPENDIX C – Consultant Professional Profile .......................................................................... 16
To: NeighborWorks America Audit Committee

Subject: Audit Review of Database Administration and Controls

Please find enclosed the final audit report on the Audit Review of the Corporation’s Database Administration and Controls.

Please contact me with any questions you might have. Thank you.

Frederick Udochi
Director of Internal Audit

Attachment

cc: E. Fitzgerald
    M. Forster
    C. Wehrwein
    J. Bryson
    T. Lyons
# Function Responsibility and Internal Control Assessment

**Audit Review of the Database Administration and Controls**

<table>
<thead>
<tr>
<th>Business Function Responsibility</th>
<th>Report Date</th>
<th>Period Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Management</td>
<td>July 26, 2013</td>
<td>June 20, 2013 to July 2, 2013</td>
</tr>
</tbody>
</table>

## Assessment of Internal Control Structure

<table>
<thead>
<tr>
<th>Effectiveness and efficiency of operations</th>
<th>Generally Effective¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability of financial reporting</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Compliance with applicable laws and regulations</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

---

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

---

¹**Legend for Assessment of Internal Control Structure:** 1. **Generally Effective:** The level and quality of the process is satisfactory. Some areas still need improvement. 2. **Inadequate:** Level and quality of the process is insufficient for the processes or functions examined, and require improvement in several areas. 3. **Significant Weakness:** Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.
# Executive Summary of Observations, Recommendations and Management Responses

<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation Summary</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation</th>
<th>Estimated Date of Implementation (Month/Year)</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the testing performed, Internal Audit noted that the Database Maintenance Procedure standards should be aligned with Corporate Retention Policies and Procedures.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Rating: (b) (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observations</td>
<td>Agreement</td>
<td>Summary</td>
<td>Recommendation</td>
<td>Accept IA</td>
<td>Response</td>
<td>Date</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>---------</td>
<td>----------------</td>
<td>----------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>Database Audit Logging and Alerting</td>
<td>Yes</td>
<td>Recommendation No: 2</td>
<td>Database Audit Logging and Alerting</td>
<td>Yes</td>
<td>Management agrees that IM should follow a risk based approach in order to increase the usefulness of information and types of events that currently being logged.</td>
<td>Q2 FY14</td>
</tr>
<tr>
<td>Based on the testing performed, Internal Audit noted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit trail mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit logging and alerting provide System Administrators and Database Administrators the ability to respond to security breaches at the database activity and transactional levels in a timely manner.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Rating:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summarized Observation; Risk Rating</td>
<td>Management Agreement with Observation (Yes/ No)</td>
<td>Internal Audit Recommendation Summary</td>
<td>Accept IA Recommendation (Yes/ No)</td>
<td>Management’s Response to IA Recommendation</td>
<td>Estimated Date of Implementation (Month/Year)</td>
<td>Internal Audit Comments on Management Response</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Observation No. 3 Schema Separation</td>
<td>Yes</td>
<td>Recommendation No. 3 Schema Separation</td>
<td>Yes</td>
<td>Management agrees</td>
<td>Q2 FY14</td>
<td>Internal Audit accepts Management’s response.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where beneficial.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>It is worth noting, database separation is already in place, due to individual application databases, and role based access permissions established within each application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Based on our inspection of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>database configurations, Internal Audit noted that</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Rating: (3) (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schemas will allow separation of database users from database object owners. They also give DBAs the ability to protect sensitive objects in the database and group logical entities together.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3) (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observation No. 4</td>
<td>Management Agreement with Observation (Yes/ No)</td>
<td>Internal Audit Recommendation Summary</td>
<td>Accept IA Recommendation (Yes/ No)</td>
<td>Management’s Response to IA Recommendation</td>
<td>Estimated Date of Implementation (Month/Year)</td>
<td>Internal Audit Comments on Management Response</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Sensitive System Privileges and Utilities</td>
<td>Yes</td>
<td>Recommendation No. 4</td>
<td>Yes</td>
<td>Management agrees with the IA recommendation and will have IM</td>
<td>Q4 FY13</td>
<td>Internal Audit accepts Management’s response.</td>
</tr>
<tr>
<td>Based on our inspection of database configurations, Internal Audit noted that unnecessary extended stored procedures had not been removed.</td>
<td></td>
<td>Sensitive System Privileges and Utilities</td>
<td>To prevent unauthorized privileged access to the database and underlying operating system, Internal Audit recommend that Stored procedures allow SQL developers and administrators to run repetitive tasks like inserting data and running queries. Extended stored procedures give functionality that is not necessarily contained within like allowing DOS commands to run and working with e-mail.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Risk Rating Legend:**

**Risk Rating: HIGH**  
A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation’s reputation.

**Risk Rating: Moderate**  
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

**Risk Rating: Low**  
A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

<table>
<thead>
<tr>
<th># Of Responses</th>
<th>Response</th>
<th>Recommendation #</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Agreement with the recommendation(s)</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>0</td>
<td>Disagreement with the recommendation(s)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Background

NeighborWorks® America (NeighborWorks) maintains [b](4) for the storage and management of data. A large majority of the databases are [b](4). The key areas of focus are user access and how they authenticate to the system to gain access. The databases are managed and supported by the Database Administrators (DBAs) within the Information Management (IM) department and the DBAs are responsible for database administration and maintaining the security of the databases. [b](4)

Objective

The audit objective was to obtain assurance on the database controls in place that would ensure compliance with IT Security Governance and industry best practices for organizations of similar size and function as NeighborWorks. In addition, the objective of this review was to ensure adequate controls were consistently maintained in databases (including configuration settings, user access controls, administrative access controls, audit logging, monitoring, authentication, and maintenance).

Scope

This audit was limited to reviewing controls for two selected databases. The two databases selected were [b](4) A risk-based sampling approach was utilized to select the two databases from the list that Information Management (IM) provided containing [b](4) databases (See Appendix A – NeighborWorks Databases). The scope for this review did not include segregation of duties and change management controls as recommendations around these issues have been previously noted in the IT Security Planning/Network Security (report dated April 15th).

Methodology

The methodology used to perform this review included the use of relevant guidelines outlined in the Control Objectives for Information and related Technology (COBIT) framework, System Administration Networking and Security Institute (SANS), International Organization for Standardization (ISO) 270001-2, Center for Internet Security (CIS) Benchmark, and the National Institute of Standards and Technology (NIST). The Corporation’s non-profit status and industry will dictate the degree to which the recommended best practices may be relevant or required. The methodology used involved the following three Phases:

Phase 1 – Information Gathering
Questionnaires – Questionnaires regarding the identification and existence of security controls in place for [b](4) databases were developed and distributed to the appropriate Information Management staff.

Walkthroughs – Interviews were conducted with the DBA to gather an understanding of the DBA administration processes and procedures. The walkthroughs permitted Internal Audit to observe, assess, and gather information regarding the operational effectiveness of the database controls in place.

**Phase 2 – Testing**

Document Review - Internal Audit reviewed the policy, procedures, and security-related documentation pertaining to the [b](4) databases. The documentation provided information about security controls that are currently in place or planned for the future.

Listed below are the types of information reviewed during the audit:

Following the collection of system characterization information, the information collected was reviewed and analyzed to gain an overall understanding of the operational effectiveness of the Information Technology General Controls (ITGCs). Internal Audit obtained and inspected a listing of security policies and procedures. Additionally, database configuration settings were inspected for compliance with CIS Benchmark and COBIT. The Confidentiality, Integrity, and Availability\(^2\) components of the database were analyzed during this Phase as well.

**Phase 3 – Reporting**

\(^2\) Confidentiality - refers to preventing the disclosure of information to unauthorized individuals or systems.

Integrity - In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle

Availability - measures information system ability to be available when it is needed.
Once the risk rating was established, recommendations were developed to enhance the tested ITGC controls. Internal Audit documented the results in this report and presented them to IM during an Exit Conference. This report describes the operational effectiveness of the tested controls and identifies observations for areas of improvement.

**Observations and Recommendations**

**Database Policy and Procedures**

**Observations # 1 – Database Maintenance Standards**

Based on the testing performed, databases are equipped with numerous auditing capabilities that could capture an immense amount of information which could ultimately impact the performance of the machines running the database, as well as overwhelm staff and the tools responsible for monitoring the logs. Audit files (logs) are however essential as they assist in the detection and analysis of the root cause of security violations. Archival procedures are designed to be aligned with the already established corporate retention policies. Maintaining audit files (logs) allows the System Administrator (SA) and Database Administrator (DBA) to properly detect, trace, and report violations.

**Recommendation # 1 - Database Maintenance Standards**

IA recommends that Information Management (IM) update the Database Maintenance Procedure to on a specified periodic basis. Management should ensure that in implementing this recommendation that the database archival and purging standards be aligned with the Corporation’s Retention Policy.

**Database Audit Logging and Alerting**

**Observation # 2 – Database Audit Logging and Alerting**

Based on the testing performed, Internal Audit noted that the Database Administrator (DBA)/System Administrator (SA) of high risk audit events. Audit logs allow an Administrator to determine a pattern of normal behavior for users and subsequently detect anomalous or malicious events that deviates from the normal behavior. Examples of such behavior include unauthorized users and changes in configuration. In the event that the audit log feature was turned off, identifying personnel who initiated the change would be difficult. It is industry standard for organizations such as NeighborWorks to maintain a continuous and auditable security monitoring procedure which includes enabling audit logs at all times.

**Recommendation # 2 – Database Audit Logging and Alerting**
Internal Audit recommends that IM deploy a risk-based approach to identify high-risk server and database audit events. Only high risk events should be included in the audit logs to avoid slowing performance. Listed below are some suggested audit events that the systems should be configured to track and monitor:

Audit logs should be secured from tampering and unauthorized access. Audit logs should be regularly reviewed and appropriately actioned. Internal Audit further recommends that IM adhere to commonly accepted best practices, which suggests that audit log files be removed from the system where they are generated and collected into a centralized log management system. They should be held for as long as the Corporation’s Retention Policy dictates before being purged. An example of a centralized log management system is a Security Information and Event Management (SIEM) archive solution which employs long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a database breach will be at the time of the breach occurring.

Internal Audit further recommends that the DBA configure alerts to inform SA and DBAs when sensitive or critical database objects are changed or modified. The mechanism should be configured to detect and notify DBAs of anomalies or malicious behavior such as unauthorized users, changing configuration options within instance configuration. This should be applied to all databases after IM has conducted a risk-based approach to identifying them. SA and DBA should ensure corrective actions are taken when an alert is raised.

Database Configuration

**Observations # 3 – Schema Separation**

Based on our inspection of database configurations, Internal Audit noted that Schemas provide a logical container to which permissions can be granted. This separation means that users can be assigned permissions to multiple objects in a schema rather than assigning rights to their user accounts. Schemas separation allows separation of database users from database object owners. They give DBA’s the ability to protect sensitive objects in the database and group logical entities together.
**Recommendation # 3- Schema Separation**

Internal Audit recommends that DBA’s assign [REDACTED] in order to prevent users from being assigned excessive rights and to ensure users are not being granted over privileged access to databases.

**Observations # 4– Sensitive System Privileges and Utilities**

Based on our inspection of [REDACTED] database configurations, Internal Audit noted that [REDACTED] provides stored procedures that may allow privileged access to the underlying operating system. [REDACTED] Stored procedures [REDACTED] developers and administrators to run repetitive tasks like inserting data and running queries. Extended stored procedures give functionality that is not necessarily contained with [REDACTED] Server, like allowing DOS commands to run and working with e-mail.

**Recommendation # 4- Sensitive System Privileges and Utilities**

To prevent unauthorized privileged access to underlying operating systems, Internal Audit recommends that DBA’s [REDACTED] Internal Audit has provided IM with [REDACTED] that should be reviewed for removal [REDACTED]

**Conclusion**

Internal Audit has provided within this report considerable recommendations to enhance the technical, managerial, and operational controls of the [REDACTED] databases. Management should also consider extending these recommendations to other databases considered to be of high risk after IM’s risk-based analysis. Management ratification of [REDACTED] database configuration settings will ensure appropriate security measures are implemented and maintained. Auditing should be enabled on all pertinent NeighborWorks [REDACTED] to detect and alert the SA and DBAs of malicious behavior such as unauthorized user and database configuration changes. The recent hiring of the IT Security and Compliance Manager will further enhance the separation of duties controls and overall support of IT Security Operations.
APPENDIX A – NeighborWorks Databases
(Selected Databases are bolded)

*Externally Hosted*
APPENDIX C – Consultant Professional Profile

(b) (4) is an IT Security consultant with over 20 years experience in IT Security and Auditing. (b) (4) has held senior consulting positions with (b) (4) auditing firms. (b) (4) has had prior work experience with NeighborWorks America as he conducted the 2007 IT Security Review. Additionally, he has conducted reviews with similar firms such (b) (4).

(b) (4) His key strength is his proven ability to work across multiple functional teams and with clients to assess, prioritize, and implement strategic business goals and IT audit objectives. He is effective is advising companies on IT security best practices and implementing IT Audit Frameworks such as COBIT. He is also a member of ISACA and holds CISSP, CSOX/P and CISO certifications.