To:       Ken Wade, Eileen Fitzgerald, Jeffrey Bryson, Michael Forster

From:  Frederick Udochi
cc:     Thomas Lyons, Mia Bowman

Date:  March 25, 2009

Subject: Review of Backup and Data Retention Management Process

Enclosed is a copy of the recently concluded review of the Backup and Data Retention Management Process. Please review and let me know if you have any comments or questions. Thanks.
**Executive Summary**

Audit Review of the Backup and Data Retention Management Process

<table>
<thead>
<tr>
<th>Business Function and Responsibility</th>
<th>Report Date</th>
<th>Period Covered:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Management, General Counsel</td>
<td>March 12, 2009</td>
<td>January 2009 through March 2009</td>
</tr>
</tbody>
</table>

**Assessment of Internal Control Structure**

<table>
<thead>
<tr>
<th>Effectiveness and efficiency operations</th>
<th>Reliability of Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Generally effective.**¹</td>
<td><strong>Generally effective.</strong></td>
</tr>
<tr>
<td>Recommendations in specific areas are noted below.</td>
<td>Recommendations in specific areas are noted below.</td>
</tr>
</tbody>
</table>

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.
Summary of Observations and Recommendations:

<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation (Received 9/1/09)</th>
<th>Estimated Date of Implementation</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Although Records Management and Retention Guidelines exist, they are not readily accessible to employees.</td>
<td>Yes. The Board adopted a Records Management and Retention Policy on March 28, 2005. The policy has not been included in the Administrative Manual. Currently, the manual is undergoing a rewrite by an outside consultant and an updated policy will be included in the new manual.</td>
<td>The Records Management and Retention Guidelines document be made available to all employees in its entirety and consolidated into a single document/location that includes all policies and procedures regarding back up and data retention.</td>
<td>Yes.</td>
<td>The Guidelines and all policies and procedures regarding back-up and data retention will be included in the new Administrative Manual. As a short term measure, the current Records Management and Retention Policy will be added as an addendum to the Administrative Manual, and the current Administrative Manual and Records Management and Retention Policy addendum will be uploaded to Inside NW.</td>
<td>Short term measure: July 2009</td>
<td>Long term: January 2010</td>
</tr>
</tbody>
</table>

The observations and recommendations in this section are summarized at a high level for informational purposes. To obtain a full, detailed explanation of each, please refer to the “Observations and Recommendations” section. Management’s response is directly related to the detailed observations and recommendations noted in the “Observations and Recommendations” section.
<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation (Received 9/1/09)</th>
<th>Estimated Date of Implementation</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. The primary vehicles to implement the Guidelines, assignment of Document Officers and annual training of the Document Officers, were not in place at the time of the review.</td>
<td>Yes.</td>
<td>Management should consider fully implementing an ongoing training program to ensure compliance with the Corporation’s Records Management and Retention Guidelines.</td>
<td>Yes.</td>
<td>Management will consult with staff development and training to determine the most effective and cost-efficient method to provide training to the Document Officers as well as publish a list a staff members assigned to this role.</td>
<td>January 2010</td>
<td>Internal Audit accepts Management’s response.</td>
</tr>
<tr>
<td>Risk rating:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Assurance that relevant electronic records are retained according to the Records Retention Guidelines could not be readily ascertained.</td>
<td>Yes. IM follows the record retention policies and backup policies as described in the Administrative manual. The only &quot;exceptional&quot;</td>
<td>Management should consider providing more detailed descriptive procedural actions that would facilitate staff guidance in the implementation of corporate policy on records management and data retention.</td>
<td>Yes.</td>
<td>Management will add detailed descriptive procedural actions that would facilitate staff guidance in the implementation of corporate policy on records management and data retention in the new Administrative Manual.</td>
<td>January 2010</td>
<td>Internal Audit accepts Management’s response.</td>
</tr>
</tbody>
</table>
Data handling at this time is the financial system backups have a longer retention timeline than everything else. (And that is specified in the manual.)

There are no specific policies currently in place that specify policies for electronic vs paper storage.
<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/No)</th>
<th>Internal Audit Recommendation</th>
<th>Accept IA Recommendation (Yes/No)</th>
<th>Management’s Response to IA Recommendation (Received 9/1/09)</th>
<th>Estimated Date of Implementation</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. The Electronic Information Storing Policy section of the Guidelines incorrectly references Section 606 of the Admin Manual, which does not address Electronic Information Storing Policy.</td>
<td>No.</td>
<td>Management should consider revising the Guidelines to reference the appropriate documentation, or remove the reference entirely.</td>
<td>Partially Accept.</td>
<td>The heading of this section can be rewritten. The reference to section 606 under the Electronic Information Storing Policy of the Guidelines refers the reader to section 606 of the Manual for the requirements of the Corporation’s operational policies and procedures related to corporate information technology and email policies and that citation is correct in that section 606 is entitled: “Corporate Information Technology: Operational Policies and Procedures.”</td>
<td>January 2010</td>
<td>Internal Audit stands by its original observation and recommendation and agrees that the heading of this section in the Records Management &amp; Retention Guidelines be rewritten since the reference does not address an “Electronic Information Storing Policy”, as inferred in the current heading’s title. Perhaps a heading which reads “Corporate IT Operational Policies &amp; Procedures” would be more appropriate for this reference.</td>
</tr>
</tbody>
</table>

Risk rating: [ ]
<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/No)</th>
<th>Internal Audit Recommendation</th>
<th>Accept IA Recommendation (Yes/No)</th>
<th>Management’s Response to IA Recommendation (Received 9/1/09)</th>
<th>Estimated Date of Implementation</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. While Data Backup, Backup Monitoring and Tape Tracking procedures appear to be in place, they are not fully documented. Additionally, evidence of daily Backup Monitoring is not kept on file to document performance.</td>
<td>Yes</td>
<td>Data Backup, Backup Monitoring and Tape Tracking procedures should be formally documented, and a process should be put in place to evidence performance of daily Backup Monitoring. Management may also want to evaluate the feasibility of tape encryption to prevent unauthorized disclosure of sensitive data in the event of a breakdown in physical security controls.</td>
<td>Yes</td>
<td>Management is pleased that IA has confirmed out backup processes are working well. Management agrees the documentation needs to be expanded and will augment the current documentation to include LiteSpeed SQL database backup and Double-Take remote server replication. Management will also document the backup monitoring/validation processes and expand documentation of the tape tracking &amp; logging processes. Management will review encryption options, requirements and the performance impact on backup/recovery activities and make a determination whether to apply such measures.</td>
<td>Oct-09</td>
<td>IA accepts Management’s response.</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>Management Response to Audit Review Recommendations</th>
<th>Backup and Data Retention Management</th>
</tr>
</thead>
<tbody>
<tr>
<td># Of Responses</td>
<td>Response</td>
</tr>
<tr>
<td>4</td>
<td>Agreement with the recommendation(s)</td>
</tr>
<tr>
<td>1</td>
<td>Disagreement with the recommendation(s) (Management has stated that they “partially agree” with this recommendation.)</td>
</tr>
</tbody>
</table>
Audit of Backup and Data Retention Management

Objective
The objective of the audit is to obtain assurance that critical systems and data are adequately backed up in compliance with prevailing data retention policies and regulations.

Scope
Backup and Retention of NeighborWorks America’s information systems and data is a critical component of the IT Infrastructure and is essential to providing the organization with high-availability applications, the ability to recover from business continuity events and the ability to comply with relevant federal and state laws regarding record retention. There must be a risk based approach to determining what systems and data require backup, the frequency, method, and the length of time such data shall be retained.

Included in our scope was a review of the risks and controls surrounding:
- Backup and Retention policies and procedures
- Backup configuration
- Retention & Tape Tracking
- Backup Security

In conducting this review Internal audit engaged the services of [name] of [name]. [Name] is a Certified Internal auditor and Certified Information Systems Auditor. (See Appendix A for Bio)

Background
A Records Management and Retention Guidelines was developed by management and approved by the Board of Directors on March 28, 2005. This document outlines the scope of the records management program and identifies responsible parties and processes for carrying out the implementation of the Guidelines. The document specifically calls for each Business Unit to assign a Document Officer (records custodian), who is responsible for ensuring that Unit’s compliance with the procedure. The Office of the General Counsel plays a supporting role by handling inquiries, providing annual Document Officer training, and soliciting feedback from the Business Units. The Guidelines also provide a Records Retention Schedule which indicates specific record types and their required retention period. In addition Information Management has developed a Data Backup Policy to document the process by which file servers, database servers, mail servers, webservers and Windows Domain Controllers are backed up to tape and sent offsite to a secure storage facility. This Data Backup process is the primary means of retaining records that are in electronic form.

We determined that the Corporation employs two types of tape backup methods at this time: Differential and Full Backup. Differential backup picks up only changes since the last backup, while Full Backup picks up the entire set of data. The Data Backup
Policy calls for Differential backups to be performed Monday through Thursday and Full backups to be performed between Friday and Sunday. Additionally, a Monthly Full backup is performed on the last Friday of the month.

Backup System configurations supporting the above tape backup schedule were obtained from Information Management as part of the review procedures. In order to gain an understanding of whether pertinent electronic records are being backed up to tape in accordance with the Records Retention Schedule, Internal Audit performed a mapping of each Record Type in the Records Retention Schedule, to the application(s) or server(s) that it could reside within. We found that all applicable applications were backed up to tape, per review of the Backup System configurations.

Once tape backups are performed, they are picked up by [REDACTED], who transports them to an offsite storage facility where they are retained according to a pre-set schedule implemented by Information Management. Backups performed Monday through Thursday are kept offsite for one week and used again upon their return to the Corporation. Backups performed on Friday or weekends are similarly kept offsite for one month and used again upon their return to NeighborWorks. The monthly tape is stored off-site for one year. The only tapes that are retained offsite for greater than one year are annual backups of the Navision system\(^3\) to capture year-end data in October. Information Management (IM) utilizes a spreadsheet to track the location of tapes as they are handed off to and returned from [REDACTED]. IM also has access to view reports of the tape inventory at [REDACTED], through the vendor’s web application.

[REDACTED] provided a description of controls in place to ensure the Physical Security of tapes while in transit and in storage at [REDACTED]. Per [REDACTED], secure tape containers are picked up by Security Service Representatives and are transported via a secure vehicle to the offsite location. The containers are then unloaded in the secure facility, under video surveillance. Security controls in place at the [REDACTED] offsite location include card key access control, alarm system, close-circuit TV monitoring and visitor controls.

Lastly, the Records Management and Retention Guidelines contain a document destruction policy that requires records (in all forms, including hard and electronic copies) to be disposed of by means appropriate to their nature or level of confidentiality, e.g., shredding, recycling or deleting, at the expiration of the specified retention period and after obtaining any necessary approvals. Except in the case of the annual backup of the [REDACTED] system, the implementation of this document destruction policy correlates more to a coordinated Business Unit effort that may require deletion of certain application records, electronic documents, emails and other forms of electronic data, rather than to destruction of backup tapes. Destruction of backup tapes is often performed simply to remove an older, and possibly less reliable, tape from the Backup and Offsite Rotation process.

---

\(^3\) The Corporation’s Financial Accounting Application System
Observations and Recommendations

1. It was observed that even though Records Management and Retention Guidelines exist, they are not readily accessible to employees. While various sections of the corporate Administrative Manual address record retention, they are not consolidated in one location, or comprehensive enough to ensure employee awareness of the full Records Management and Retention Guidelines.

Recommendation:

It is recommended that the Records Management and Retention Guidelines document be made available to all employees in its entirety and consolidated into a single document/location that includes all policies and procedures regarding back up and data retention. In addition to the current retention and destruction policy documents identified, consideration should be given to archival procedures, up to date evidentiary standards, document reproduction tests, online storage repositories, record custodians and a destroyed documents “log book”.

2. It was observed that the primary vehicles to implement the Guidelines, assignment of Document Officers and Annual training of the Document Officers, were not in place at the time of the review and as a result there was no means of ensuring compliance with the Guidelines in that aspect.

Recommendation:

We recommend that management fully implement an ongoing training program to ensure compliance with the Corporation’s Records Management and Retention Guidelines. This would include employee awareness initiatives, identification of responsible parties, employee electronic data storage as well as ongoing compliance monitoring within the context of the current guidelines or for any subsequent modifications or versions developed.

3. It was also observed that while critical applications are included in the tape back up process, the assurance that relevant electronic records are retained according to the Records Retention Guidelines could not be readily ascertained. Electronic records which can take the form of application data, emails, Word documents, spreadsheets, PDF documents and scanned images might require manual intervention to ensure their archival. This could be inadvertently overlooked by the individual employee and possibly lead to loss of such records. The lack of a formal procedural process that would inform employees of how to execute this compliance within the Guidelines further compounds this issue. In effect we observed that:

- There is no formal procedural information requiring financial spreadsheets and other electronic documents that require retention, be stored on a file

---

4 A requirement of the Records Management and Retention Guidelines
server rather than a local hard drive, to ensure inclusion in the backup process.

- There is no formal guidance instructing email users on how to store relevant emails that may be required to be retained. Outlook Personal Folders can be configured by the user to store messages on the user’s PC hard drive or on a file server directory. Storage on the file server directory would ensure inclusion in the backup process.

**Recommendation:**

We recommend that management provide more detailed descriptive procedural actions that would facilitate staff guidance in the implementation of corporate policy on records management and data retention. This could include procedures detailing how to appropriately archive electronic emails and documents such as critical Word and Excel spreadsheet files. This would make individual employees more cognizant of the fact that these documents must be stored on a network file server, in order to be included in the formal backup process.

4. The Guidelines document contains an incorrect reference to another document. Specifically, the Electronic Information Storing Policy section of the Guidelines refers to Section 606 of the Administrative Manual, which does not address Electronic Information Storing Policy.

**Recommendation:**

We recommend that management revise the Guidelines to reference the appropriate documentation, or remove the current reference entirely.

5. While Data Backup, Backup Monitoring and Tape Tracking procedures appear to be in place, they are not fully documented. Additionally, evidence of daily Backup Monitoring is not kept on file to document performance. Documented procedures are necessary to ensure continuity in the event of staff turnover (termination/transfer), reorganization or business continuity situations.

- The Data Backup Policy currently addresses the ARCServe backup process, however does not document LiteSpeed SQL database backup or Double-Take file server replication from remote sites.
- A documented Backup Monitoring procedure does not exist at this time. This document should cover the scope, frequency and responsible individual for backup monitoring, escalation procedures for failed backups, and documentation of performance.

---

5 ARCServe is a software program that backs up server software and data to tape. Litespeed is a software program that backs up databases to a centralized server, for inclusion in the ARCServe tape backup process. Doubletake is a software program that replicates data on file servers at remote NeighborWorks offices, to a centralized server at DC headquarters, for inclusion in the ARCServe tape backup process.
• A documented Tape Tracking procedure does not exist at this time. This document would cover the tracking of tapes from pickup to return to NeighborWorks.
• Although physical security controls appeared adequate to prevent unauthorized parties from accessing the tapes, if there were to be a breakdown in one of these security controls, tape data is not encrypted at this time.

Recommendation:
It is recommended that the Data Backup, Backup Monitoring and Tape Tracking procedures be formally documented, and a process put in place to evidence performance of daily Backup Monitoring. Management might also want to evaluate the feasibility of tape encryption to prevent unauthorized disclosure of sensitive data in the event of a breakdown in physical security controls.

Conclusion

Information Management has taken into consideration the risks associated with Data Backup and Record Retention and have for the most part created policy accordingly. Additional coordination to ensure effective implementation of the Record Retention policy with regards to electronic records should be undertaken by the Corporation’s management. The foregoing recommendations made originate from a corporate governance standpoint with management being the primary champions. As a result the majority of these recommendations would have to be championed by management with support from Information Management.

We would like to extend special thanks to the Information Management Team for their diligent assistance during our review.
APPENDIX A

Professional Background of External Consultant

The founder of [company name] has over 8 years of experience in the IT Audit, Security and Assurance fields. His audit experience began at KPMG where he provided IT Audit and Security services in support of financial audits and consulting engagements, to clients in the private, non-profit and federal sectors. He moved into the Internal Audit profession taking on the role of Sr. IT Auditor and then Operations Audit Manager at CitiFinancial, a subsidiary of Citigroup. During his time in an Internal Audit role, he obtained a thorough working knowledge of how to evaluate technology risk, and how to effectively work with management to ensure reasonable controls were implemented.

In 2005, he moved back into the consulting field and spent nearly two years at Legg Mason, where he served in a Sr. Project Manager role in support of their Sarbanes Oxley 404 technology compliance efforts. He managed a team of 12 Internal Audit and Big 4 consultants to ensure internal SOX compliance audits were performed on time and on budget, and was also responsible for resource planning, budgeting, sampling methodology development, reporting to the Internal Controls Committee and training and mentoring staff.

Upon completion of that project, he founded [company name] a firm specializing in IT Audit & Assurance consulting, where he continues to service his existing network of Fortune 500 Internal Audit departments, Office of Inspector Generals, and CPA firms with high-quality consulting services.

He has a Bachelor of Science degree in Management Science & Information Systems, from the Pennsylvania State University, where he graduated with High Distinction. In 2002, he obtained the Cisco Certified Network Associate (CCNA) certification, demonstrating technical competence in the field of network engineering. He also currently holds the Certified Information Systems Auditor (CISA) and Certified Internal Auditor (CIA) designations.