OBM | Office of Internal Audit

Department of Commerce

Division of Financial Institutions Audit

Audit Period: April 1, 2014 through October 31, 2014

Results Summary:

Objective	Conclusion
Document Imaging and Handling Process	Well-Controlled with Improvement Needed
Maintenance and Accessibility of Electronic Records	Improvement Needed

Report number: 2015-COM-03 **Issuance date: December 18, 2014**

Executive Summary

Background

The Division of Financial Institutions (DFI) regulates state chartered financial institutions and consumer finance companies. The Division charters depository institutions, licenses non-depository financial services, and conducts on-site examinations. All examinations, supervision, and regulatory activities are performed by Division staff that specializes in the operations of each of the specific industries. The Division's Office of Consumer Affairs works to provide education to Ohioans regarding borrowing and related financial topics.

The Division has recently implemented, and continues to enhance, processes to electronically store all records.

During the audit, OIA identified opportunities for Department of Commerce to strengthen internal controls and improve business operations. This audit conforms to the *International Standards for the Professional Practice of Internal Auditing*. OIA would like to thank Department of Commerce staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the DFI's electronic records management processes. This work was completed between October and December 2014. The scope of this review included DFI's processes for retaining records electronically and in accordance with federal and state record retention policies for the Banks and Savings Institutions section, including Banks, Savings & Loan Institutions, and Money Transmitters.

The objectives of the review included the following:

- Evaluate the design and effectiveness of controls over the imaging and handling processes of key documents.
- Evaluate the design and effectiveness of controls over the maintenance and accessibility of electronic records.

The scope did not include a review over general controls of the IT systems.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Record Retention

An effective records retention policy should outline the process for creating an electronic record from a physical source, and also the process for eliminating the source document once an electronic version has been created, and has been confirmed to be a proper representation of the original source document.

The Banks and Money Transmitter sections of the DFI receive documentation via hard copy and electronic mail. DFI staff scans or uploads the documentation into Intellivue, an electronic depository intended to replace the long-term storage of physical documents. However, DFI does not have a policy in place to outline the process for destroying the original hard copy documents or deleting original electronic records once they have been electronically imaged and saved to Intellivue. DFI also does not have procedures in place to ensure that electronic documents are deleted from Intellivue, from shared drives, and from archived email storage once the required retention periods have expired.

Retaining physical documents after they have been converted to electronic records and retaining electronic records on shared drives and in email storage is an inefficient use of resources, and also presents additional opportunities for documents with sensitive or confidential information to be compromised.

Recommendation

Develop and implement a timeframe and process for destroying or deleting source documents once they have been uploaded into Intellivue. Develop policies and procedures to document the process for identifying electronic documents that reach the end of record retention periods to ensure documents are timely and appropriately deleted.

Management Response

The Division is in the process of migrating to an electronic records management system. The Division currently has a process for destroying source documentation but does not have a written policy. The Division will develop and implement a policy that includes a timeframe and a process for destroying source documentation. Additionally, the Division will work with Department Information Technology Group to review the functionality within Intellivue and implement where

practical any features that provide for a "tickler" system for records retention purposes. The Division will also review existing record retention schedules in conjunction with data maintained on network drives.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Deputy Superintendent, Division of Financial Institutions	April 2015

Observation 2 – Emailing Sensitive Information

Sensitive electronic and physical records must be properly safeguarded.

The Banks and Money Transmitter sections of the DFI electronically save both electronic and hard copies of documents to Intellivue and to shared network drives. Both Intellivue and the shared network drives' access are appropriately limited to only those users that require access. However, the Banks section routinely sends emails to field agents with the sensitive electronic records that are saved to both Intellivue and to the shared drive. DFI staff stated emails containing sensitive documents are encrypted. According to DFI staff, sending sensitive documents via email to field agents has been necessary due to limited or non-existent network access in remote areas, making accessing documents on Intellivue or shared drives difficult or impossible. Additionally, state agencies are moving towards utilizing Microsoft Office 365 cloud based email which is operated by a third party vendor that could have the potential of accessing email data.

Sending emails containing sensitive documents that are appropriately stored elsewhere increases the likelihood that records are accessed by unauthorized users and that sensitive information is compromised. Additionally, storing electronic records in multiple locations may lessen access control functionality, as access permissions may not be consistent across all locations.

Recommendation

In the short-term, determine a method for field agents to remotely access documentation from the shared drives or Intellivue, and eliminate the process of sending documentation via email.

The following are some solutions to consider:

- Work with the agency Information Technology Group to evaluate whether utilization of the agency applications (for example, a secured SharePoint site or Tumbleweed) for the transfer of documents would be a viable solution or if there are additional methods

utilized by other Divisions that can be considered.

- If DFI field agents have difficulty accessing records on the agency server, as a last resort, have agents save documents to an agency-issued portable encrypted drive, such as an Iron Key flash drive or encrypted laptop, prior to travelling to a location where network access is known to be slow or unavailable. Have agents save documents to a laptop hard drive prior to travelling, provided that the drive is properly encrypted and secure.
- Create a policy with timeframes for deleting documents from hard drives and/or wiping Iron Key flash drives within a reasonable period of time. Consider any federal stipulations over records maintenance and accessibility when creating a policy.

For a long-term solution, explore further the functionality within Intellivue to assess whether field agents can successfully access documents through Intellivue. Consider systems upgrades or training opportunities, if necessary, to ensure that all staff can efficiently and effectively utilize Intellivue. Additionally, consider exploring other business process applications that have the capability of working in a disconnected state and the ability to successfully sync to the full application when agents are able to connect to the system network.

Management Response

The Division is in the process of migrating to an electronic records management system and must adhere to high data security standards as required by Ohio Revised Code, the Federal Deposit Insurance Corporation and the Federal Reserve Bank. It should be noted that in using email as a more efficient means of document management, the Division believed emails between state employees were transmitted securely. We now understand that emails and related attachments sent between state employees may not be secure, which represents a concern for the Division.

The Division will implement written policies and procedures to address the concern regarding emailing confidential supervisory documents and the storage of such documents in multiple locations. Additionally, the Division will work with the Information Technology Group (ITG) to explore the viability of providing remote users with secure access to Intellivue, including the deployment of web based or VPN SSL access or increased use of FTPS (Tumbleweed). Further, the Division will continue to work with ITG to improve network drive access and reliability for remote users. Lastly, the Division will work with ITG to determine and evaluate the viability of other secure document sharing solutions, i.e. SharePoint.

Agency CIO Note: DAS OIT should also provide the Division with acceptable security assurance statements, or its copies of such statements with Microsoft, related to DAS OIT mandated Office 365 service prior to the implementation in March 2015.

Risk*	Remediation Owner	Estimated Completion Date

Moderate	Deputy Superintendent, Division of Financial Institutions	March 2015

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Refer to Appendix A for classification of audit observations.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee