OBM | Office of Internal Audit

Department of Commerce

Industrial Compliance Audit

Audit Period: July through December 2014

Results Summary:

Objective	Conclusion
Elevator Permitting and Operating Certification	**Improvement Needed**
Boiler Permitting and Operating Certification	**Improvement Needed**

* Refer to Appendix A for classification of audit objective conclusions.

Report number: 2015-COM-01 **Issuance date: March 26, 2015**

Executive Summary

Background

The Division of Industrial Compliance & Labor (DIC) reviews and approves the building plans for the construction and renovation of commercial and public building projects. The Division also provides regulatory certification and inspection of boiler and elevator systems essential to public welfare and safety. DIC staff members conduct inspections of plumbing, electrical and structural systems; elevators; boilers; bedding and upholstered products. Additionally, DIC provides testing, certification, licensing and continuing education services for numerous skilled trades in Ohio's building industry. The Bureau of Wage and Hour Administration within DIC administers and enforces Ohio's prevailing wage, minimum wage, overtime and minor labor laws. Ohio's prevailing wage law requires public authorities to pay the local prevailing rate of wages for work performed under public construction contracts.

The DIC works with:

- The Board of Building Standards, which sets the building code for the State of Ohio and provides training and certification for local building authorities across Ohio.
- The Board of Building Appeals, which hears requests for variance from the Ohio Building Code.
- The Ohio Construction Industry Licensing Board, which provides testing and licensure of occupations regulated to the commercial construction industry.

During the audit, OIA identified opportunities for the Department of Commerce (COM) to strengthen internal controls and improve business operations. OIA conforms to the *International Standards for the Professional Practice of Internal Auditing*. OIA would like to thank COM 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 DIC’s licensing and permitting processes. This work was completed between December 2014 and March 2015. The scope of this review included DIC's key processes related to elevator and boiler permitting and operating certifications. The scope does not include professional licenses for inspectors or operators.

The objectives of the review included the following:

- Evaluate the design and effectiveness of controls over the elevator permitting and operating certification processes.
- Evaluate the design and effectiveness of controls over the boiler permitting and operating certification processes.

Additionally, OIA performed data analysis over elevator and permitting activity during the audit period. Results were provided to management in a separate communication.

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 – Credit Card Payment Processing

Credit card information is considered sensitive data and presents a risk of credit card fraud. Consequently, an entity should implement controls surrounding the receipt, retention and processing of credit card information. Industry best practice is the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

The DIC accepts credit card payments from elevator and boiler customers for permits and certificates of operations fees. However, the DIC does not have sufficient internal controls in place to safeguard credit card information. For example, customers may fax credit card information, including the card number, expiration date, name on card, security code, and billing zip code to a fax machine that is located in a secured and locked room. However, a fiscal account clerk removes the credit card information from the secured room and carries it to her desk in order to enter card numbers into the credit card machine. Also, the DIC staff receives credit card information from customers via the US mail, email, and over the phone. The DIC staff delivers credit card information to fiscal accounts receivable staff to enter card numbers into the credit card machine. Additionally, the DIC uses several forms to collect credit card information, as well as applications and invoices that do not consistently direct customers to submit credit card information to the secured fax. One application even directs customers to submit credit card information via email or to the general fax line.

Failure to properly safeguard credit card information increases the likelihood that sensitive card information is lost, stolen or compromised, thus increasing risk to DIC. Just one incident of compromised credit card information can result in a damaged reputation to the DIC and the state of Ohio.

Recommendation

As a long-term solution, implement the required upgrades to the DIC's AMANDA system so that customers may pay fees online with a credit card to eliminate the need for the DIC or fiscal accounts receivable staff members to receive, process, or retain sensitive credit card information. COM is currently in the process of upgrading the AMANDA system to eventually include online payment capabilities. COM anticipates implementing the necessary upgrades to the AMANDA system by the end of calendar year 2015.

As a short-term solution, design and implement controls to sufficiently safeguard credit card information. For example:

- Immediately cease accepting credit card information via unsecured fax, email, or over the phone;
- Update language on credit card forms as well as applications and invoices to direct customers to submit credit card information only through the secured fax machine;
- Consider moving the credit card machine and a phone to the secured fax room so that credit cards may be processed without carrying sensitive information outside of the secured room;
- Securely destroy credit card forms containing sensitive data after processing the card number and retain only the credit card receipt that displays the last four digits of the card number as evidence of the transaction; and
- Periodically review access to the secured room to verify access is limited to accounts receivable fiscal staff members.

Additionally, management should consider exploring and assessing the viability of leveraging existing online payment functionally used within the agency as well as other state agencies.

Management Response

COM's short-term resolution:

1. We will instruct the division to direct customers to send their credit card information to our secured fax, as well as direct all phone calls for customers with credit card information to our Accounts Receivable (AR) staff. We will also notify customers that we will no longer accept credit card information by email. Should DIC staff directly receive unsolicited credit card information (via phone, U.S. mail or email), DIC staff will: forward the communication to fiscal for processing and thereafter immediately destroy the communication, and will send the customer a separate message informing them of the

proper means of processing credit card payment. This will be implemented immediately.

2. We will work with the Information Technology Group (ITG) to update applications and other documentation that goes out to customers to include the AR customer service phone number, as well as the secured fax number. We will work toward implementing by end of calendar year 2015.
3. While we acknowledge there is a risk with current location of our credit card machine, we feel this risk is minimal and accept the risk. The current location of the machine is our customer service counter, and removing this along with the staff person would negatively impact our providing customer service to the division.
4. In association with the changes mentioned before to other forms, we will be standardizing our credit card information form so that we can tear off the bottom of the form that contains the credit card information and destroy it securely. This can be implemented by July 1st.
5. While we feel that our current locked room is sufficiently secure to house our safes, as well as the secure fax that receives credit card information, we will investigate the cost of obtaining a card reader for the door. If we feel it is cost effective to change the locking mechanism, we will move forward with that.

COM's long-term resolution:

COM is moving toward an online payment portal to work in conjunction with the AMANDA database system for all DIC payments. We feel this will greatly reduce the manual payment entry of credit cards, but we will continue to accept credit card payments outside of the online portal to continue to provide customer service to Ohioans. The AMANDA system will be upgraded within the calendar year 2015. Once the upgrade takes place, the next step is to implement the payment portal to work with the upgrade.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Assistant CFO	March 2016

Observation 2 – Check Logging and Timeliness of Deposits

An effective business process for collecting revenues includes logging and documenting incoming cash and checks and reconciling checks received to checks deposited. The check handling process should be documented in policies and procedures that define roles and responsibilities. Additionally, Ohio Administrative Code section 113-1-02(A) requires state agencies to deposit all monies collected within three business days of receipt by a state entity into the state treasury.

The COM's Fiscal division receives hundreds of checks daily from the DIC customers as fee payments for permits and inspections as well as for issuing and renewing certificates of operation. Policies and procedures do not exist to define roles and responsibilities for receiving checks and to outline processes to ensure that all checks received are timely and completely deposited. In addition, testing results revealed the following:

- From a sample of ten elevator permit application fees received from July through December 2014, DIC received permit fee payments in the form of checks from four customers (the remaining customers paid the fees via credit card); however, COM staff had documentation of check receipt dates for only three of the four checks. For those three checks, COM did not deposit funds collected within three business days of receipt. Instead, funds were deposited between four and five business days of receipt.
- From a sample of eight boiler permit application fees received from July through December 2014, DIC received permit fee payments in the form of checks from all eight customers. However, COM staff had documentation of check receipt dates for only six of the eight checks. For those six checks, COM did not deposit funds collected within three business days for three (50%) of the deposits. COM deposited funds for these three checks to the state treasury four days after receipt.
- From samples of 15 elevator certificates of renewal invoices and 15 boiler inspection invoices for the period July through December 2014, COM received ten checks from elevator customers and 13 checks from boiler customers. However, COM did not log or record the receipt dates of any checks to verify timely and complete deposits to the state treasury. OIA could not confirm whether COM deposited these funds within three business days.

Failure to log all checks received, reconcile checks received to checks deposited, and have policies and procedures in place for receiving checks increases the likelihood that checks are lost or stolen without detection or that checks are not deposited to the state treasury timely.

Recommendation

Develop and implement processes to log checks when received in order to reconcile checks received to checks deposited and also confirm the completeness and timeliness of deposits. Due to the large volume of checks received, evaluate the costs and benefits of receiving payments electronically through either an online automated clearing house (ACH) system or through a lockbox service. As a long-term solution, implement the required upgrades to the AMANDA system so that customers may pay fees online to reduce the number of checks received.

Develop and implement policies and procedures for handling checks to allow compliance with

the Ohio Administrative Code to deposit receipts within three business days. Policies and procedures should describe key controls in the process, the objectives of key controls, descriptions of control functions, and positions responsible for performing functions. Periodically review policies and procedures and update as needed. Additionally, consider making appropriate changes to current processes which are at risk for not meeting the three-day deposit rule.
Management Response
COM fiscal currently has policies and procedures for processing mail, as well as posting check payments. The policies also outline the requirements for depositing to the TOS within a three day time frame.   We currently have a practice in place that if we are unable to process all of DIC payments within a three day period of time, especially during large renewal periods, we implement a voluntary overtime shift for anything that falls past four days, and implement a mandatory overtime shift for anything over five days. COM acknowledges the risk involved with not logging the checks as they are received; however, due to staffing, the volume of checks, and limitations of the database, we are currently not able to implement changes to this process. However, we feel that by moving toward an online payment portal of all DIC payments, this will help to decrease the number of checks that come into our office to manually post; thereby, decreasing this risk in the future.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Assistant CFO	March 2016

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