

**METROPOLITAN GOVERNMENT OF  
NASHVILLE AND DAVIDSON COUNTY**

**OFFICE OF INTERNAL AUDIT**

**Professional Audit and Advisory Service**

**FINAL REPORT**

**Audit of the Department of Codes and  
Building Safety**

Date Issued: September 29, 2009

Office Location and Phone Number

222 3<sup>rd</sup> Avenue North, Suite 401  
Nashville, Tennessee 37201

615-862-6110

*The Office of Internal Audit is an independent audit agency reporting directly to the  
Metropolitan Audit Committee*

**EXECUTIVE SUMMARY**  
**September 29, 2009**

Results in Brief	Recommendations
<p>We performed an audit of the processes and controls in place pertaining to the operations of the Department of Codes and Building Safety. Key audit objectives and conclusions are as follows:</p> <ul style="list-style-type: none"> <li>• Does the Department ensure inspectors are fully qualified to discharge their duties and protect public safety?  Yes. Current policies and procedures were designed to ensure inspectors were experienced, certified, and qualified.</li> <li>• Does the Department have procedures in place to ensure the validity and completeness of reviews prior to issuance of a building permit?  Yes. The current procedure was functioning as designed No material weaknesses were observed.</li> </ul> <p>Additionally, we conducted a review of the processes and controls pertaining to the KIVA application. Audit objectives and conclusions pertaining to this review are as follows:</p> <ul style="list-style-type: none"> <li>• Is the KIVA application protected from accidental and/or intentional damage to system assets (general controls)?  Generally yes. Although current procedures were functioning, we noted several areas that require improvement (see Observations A, B, and C.)</li> <li>• Does the Department have procedures in place to ensure revenues are correct and complete and KIVA transactions are reconciled with Finance EnterpriseOne information?  Yes. No material weaknesses were observed.</li> </ul>	<p>Key recommendations of this report include:</p> <ul style="list-style-type: none"> <li>• Determine requirements to enable compliance with Payment Card Industry Data Security Standards.</li> <li>• Provide an enhanced trade inspection customer complaint response process.</li> <li>• Initiate a well defined service level agreement with Metro Information Technology Services.</li> <li>• Perform a thorough information system security risk assessment process.</li> <li>• Enhance the computer system application security procedures.</li> </ul> <p>Management's response can be seen in Appendix A, page 18.</p>

## TABLE OF CONTENTS

INTRODUCTION.....	1
BACKGROUND .....	1
FINANCIAL INFORMATION.....	3
INFORMATION TECHNOLOGY BACKGROUND .....	3
OBJECTIVES AND CONCLUSIONS.....	7
A – Determine Compliance Requirements for Payment Card Industry Data Security Standards.....	12
B – Initiate a Well Defined Service Level Agreement with Metro ITS .....	12
C – Conduct a Thorough Computer/Information Systems Security Risk Assessment .....	13
D – Enhance the Computer System Monitoring Procedures .....	14
E – Improve the Customer Complaint Tracking Process.....	15
STATEMENT OF COMPLIANCE WITH GAGAS.....	17
SCOPE AND METHODOLOGY .....	17
CRITERIA .....	17
STAFF ACKNOWLEDGEMENT .....	17
APPENDIX A. MANAGEMENT RESPONSE.....	18

# INTRODUCTION

## AUDIT INITIATION

As part of the annual Audit Work Plan, the Office of Internal Audit conducted an audit of the Department of Codes and Building Safety. The basis for conducting this audit was due to the impact this organization has on protecting the lives and safety of the public.

## BACKGROUND

The Department of Codes and Building Safety was created by the Mayor and Council on July 2, 1963, by Ordinance No. 63-36. The Department of Codes and Building Safety is responsible for the interpretation, administration, and enforcement of the Metro Building Code, Property Standards Code, and Zoning Code. The Department of Codes and Building Safety is principally composed of eight distinct divisions: (1) Administrative, (2) Plans Examination, (3) Building, (4) Electrical, (5) Gas/Mechanical, (6) Plumbing, (7) Property Standards and Zoning Inspection, and (8) Permits and Zoning. The Director, who serves as the Building Official, oversees a staff of approximately one hundred employees, and supports six related licensing and appeals boards.

The Department's task is to protect the lives and safety of the public, preserve the City's quality of life, and contribute to the City's economic development. To meet these tasks, the Department conducts inspections and code enforcement activities on construction, alteration, repair, and demolition of structures to ensure that these buildings, residences, and public gathering structures are safe to occupy. This is distinctly stated in the Department's mission statement which is, "to provide permit, inspection, enforcement, and information products to the Nashville community so they can experience safe buildings and improved quality of life."

The main operation of the Department of Codes and Building Safety involves the issuance of building permits for residential, commercial and industrial constructions. The two main processes for building are permit tracking and inspection tracking. The permit tracking process begins with an application for a building permit and ends with the issuance of a building permit. The inspection tracking process commences when the building permit is issued and ends when the builder receives a Use and Occupancy Certificate.

Being the primary authority for administering the Metro Zoning Code and Building Code, the Department of Codes and Building Safety strives to become the central hub for other agencies with an interest in the permit process such as Public Works, Water Services, Fire Marshall, Health Department, Historical Commission, Metropolitan Development Housing Authority, and others. Communication between these groups is through a common computer system called KIVA. The items below describe the general

nature of the primary divisions that comprise the Department of Codes and Building Safety.

#### Administration

The Administration Division is responsible for cash receipts and processing, budgeting, human resource liaison activities with Metro Human Resources, civil service investigations, interviewing and hiring, purchasing, licensing of trade contractors and associated boards, and serving in the role of advisor to the Department Director regarding fiscal, personnel, administrative, and operational matters.

#### Plans Examination

The Plans Examination Division is responsible for reviewing commercial and industrial plans for compliance and completeness using the standards set forth by the International Building Codes established by the International Code Council. The staffs perform their work using a reference checklist from the International Building Codes. This section reviews and comments the plans in accordance with the codes while the builders/owners are working on sign-offs required by other agencies to get the building permit.

#### Inspections Division

The Inspections Division is responsible for the provision of building, plumbing, electrical, mechanical/gas, and property standards inspections in accordance with the Metropolitan Code of Law and those of the International Code Council, Inc. The Division also reviews plans submitted by permit applicants, and makes required changes to these plans and enforces the conformance to the Metropolitan Code of Law and specifications.

#### Zoning

The Zoning Division primary responsibility is for the interpretation, administration and enforcement of the Metro Zoning Code. This Code includes Metro's landscaping, buffering, and tree replacement requirements. The Division is also responsible for the review and issuance of zoning permits applications, informing the public regarding the zoning code and maintaining current and permanent records relating to the adoption, amendment, administration and enforcement of the Zoning Code. The Division also supports the activities of the Board of Zoning Appeals and enforces the actions of that Board, and subsequently reviews plans submitted by applicants to determine which of Metro Nashville's various agencies are required to review plans prior to permit issuance.

The Urban Forester functionally reports to the Zoning Administrator and is responsible for the review of landscape plans and the enforcement of the Tree and Landscape Ordinance. The Division's focus is the protection of existing trees and the continued planting of quality trees within the Metropolitan area. An approved landscape plan is required prior to the issuance of a building permit for developments other than single family or duplex residences.

#### Property Standards

The Property Standards Division is primarily responsible for the enforcement of the Metro Property Standards Code and the Metro Zoning Ordinance in

connection with Metro building permits and associated Use and Occupancy Certificates. The Property Standards Division also enforces the Metro Sign Ordinance. They further investigate Property Standards Code and Zoning Code violations, and have been assigned responsibility for handling abandoned vehicles on public streets.

## FINANCIAL INFORMATION

Comparative financial information, in summary form, can be seen below in Exhibit A.

### Exhibit A – Codes and Building Safety Department Comparative Financial Information

	Fiscal Year End 2007	Fiscal Year End 2008	July to December 2008
<b>Revenues</b>	\$11,788,328	\$10,293,338	\$3,474,767
<b>Expenditures</b>	7,793,472	7,985,941	3,752,431

## INFORMATION TECHNOLOGY

### KIVA System

The KIVA software is a developmental management system used for many land related activities within the Metro Government. It includes four integrated modules (Land, Professionals, Permitting, and Request for Service/Violation tracking.) It was acquired in September 2003 to replace the then existing mainframe system used for land, permitting and violation tracking. The KIVA system is one of several products supported by the Accela Corporation and Metro's implementation includes several Accela branded products integrated with KIVA. The Department of Codes and Building Safety uses KIVA's developmental management system, geographical information system integrated map display, wireless (tablets in the field for inspectors), interactive voice recognition (phone requests for inspections), and KIVANet/KIVACitizen (web inquiry/web permit application, payment, and issuance) functionality.

KIVA is presently deployed by the Codes and Building Safety, Public Works, Water Services Connections and Water Services Storm Water Departments to issue and track permits and inspections. The Property Assessors', Planning, and Public Works all use KIVA to manage land, property ownership, zoning, and streets. The Department of Codes and Building Safety, specifically the Property Standards Division, also uses it for recording and tracking violations and violations inspections. Planning is scheduled to begin using KIVA for Planning permits in the near future. As many as 15 other Metro departments use KIVA for querying permits and signing-off permit related activities. Additionally, KIVA land and permit information is used in several public inquiry and geographical information system applications. Also the Beer Board, Taxi Wrecker, and Health Departments

have expressed interest in using KIVA to track permits, licenses and violations.

KIVA data is pushed to other department's systems, especially the Assessor's Patriot appraisal system, the Trustee's Manatron Tax Billing system and Public Works' CityWorks work order system through periodic data loads and nightly changed record interfaces. KIVA data is also shared with Nashville Electric Services, Piedmont Natural Gas, and other geographical information system users through periodic interface updates.

#### EnterpriseOne Interface

Automating the KIVA daily deposit to the Finance Department's EnterpriseOne financial system was developed by KIVA (in cooperation the Finance Department) using a standard input file format. Due to KIVA's permitting function, it has an extensive cashiering and balancing process. KIVA handles multiple payment types and cashiers, assigns unique receipts to payments, allows voids and other adjustments (with appropriate supervisor security) and records all financial activities for ease of balancing. KIVA fees and payments are stored in a number of tables in the KIVA system. KIVA allows multiple fees per permit and multiple payments per fee. A simple trade permit might have five fee details resulting in five fee detail payment records.

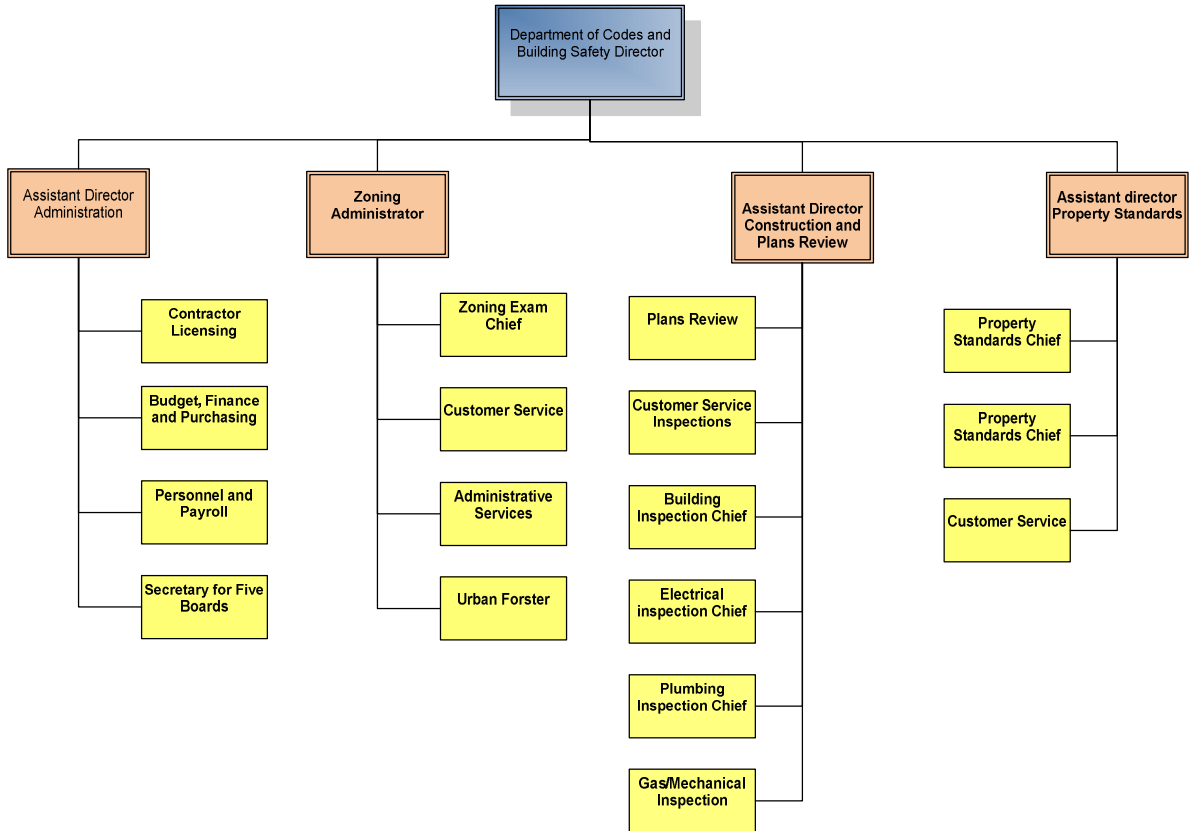
#### Buzzsaw

Buzzsaw is an internet-based software product created by Autodesk and designed to provide electronic plans submission and concurrent electronic plan review. Concurrent plan review allows all pertinent departments, involved in the review process, to review and comment on the same set of construction documents within the same time frame. The system works by allowing the customer to send electronic files of construction documents (blueprints) to a web address and subsequently loading these non-modifiable files into the distribution program. Using the distribution program, all departments involved can review, make comments, and mark-up the files. Moreover, each involved department can then see the comments and revisions requested by other departments, thus improving communications and coordination. Additionally, the system allows the customers to view the status of the plan reviews and the comments online.

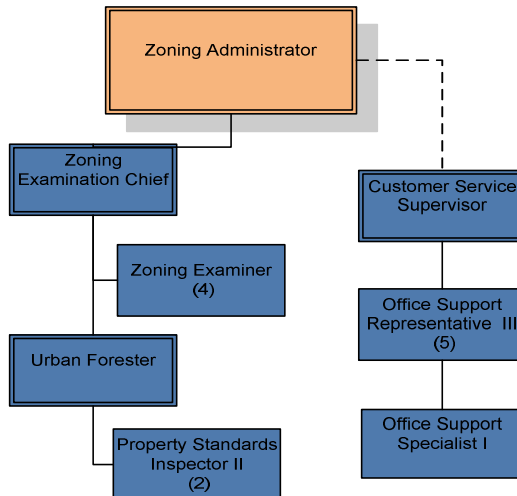
# ORGANIZATION STRUCTURE

## Exhibit B - Department of Codes and Building Safety Organizational Structure

### Department of Codes and Building Safety

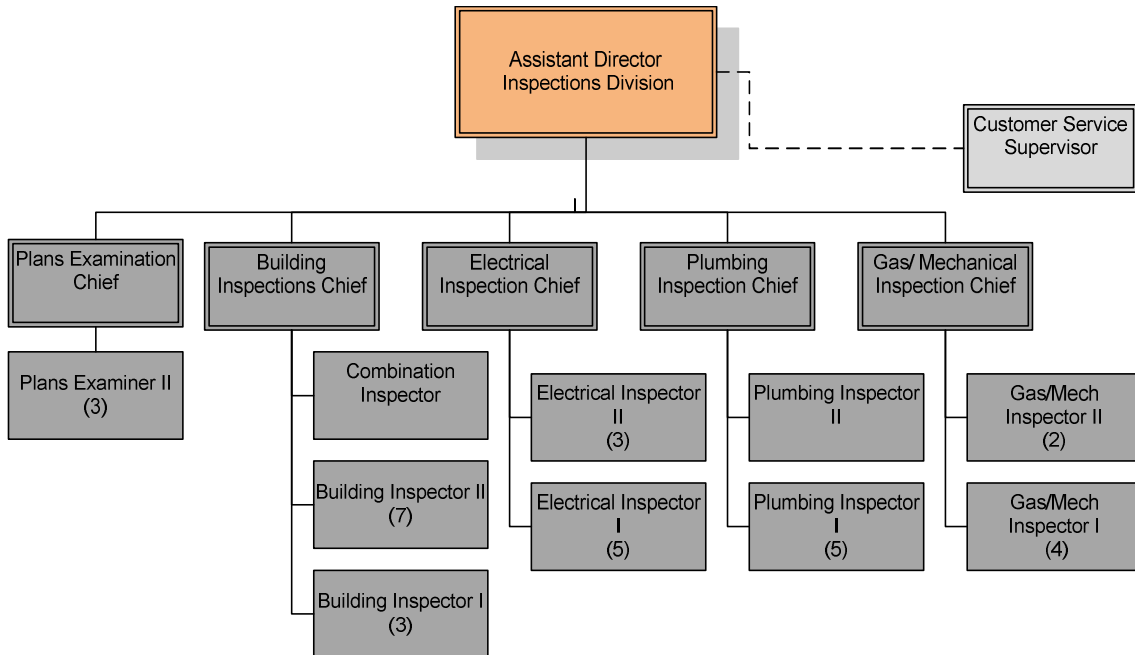


### Zoning Division

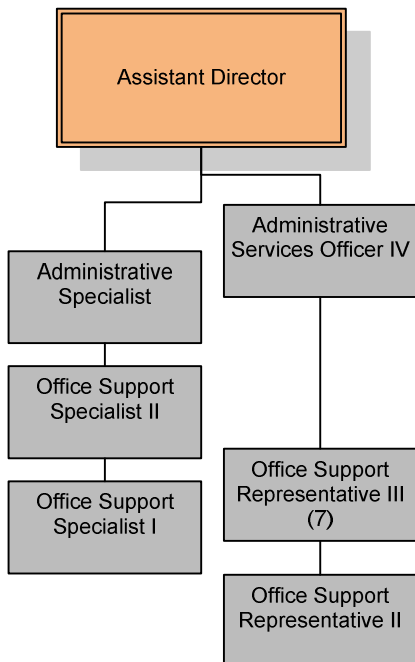


**Exhibit B (continued) - Department of Codes and Building Safety  
Organizational Structure**

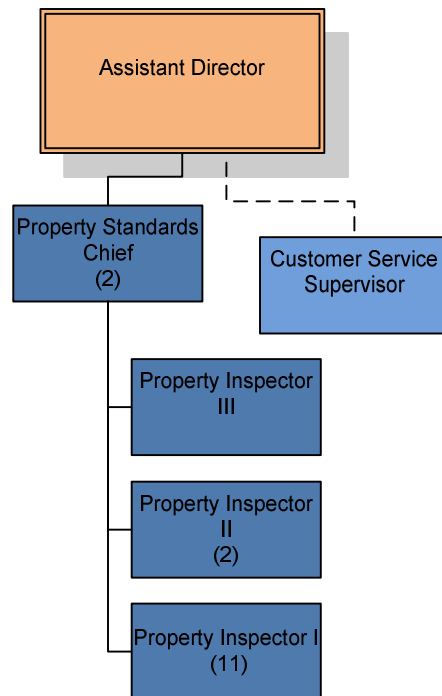
**Inspections Division**



**Administration**



**Property Standards**



## OBJECTIVES AND CONCLUSIONS

1. *Does the Department of Codes and Building Safety have procedures in place to prevent inspector bribery or inspection favors for select contractors?*

Generally yes. The Office of Internal Audit evaluated the Department's procedures to ensure that risk of inspector bribery or inspectors favoring particular contractors were minimized, if not eliminated. We performed test of controls to ascertain whether Department of Codes and Building Safety personnel, those required to sign the Metro-wide financial disclosure forms, have complied with the requirement. The Office of Internal Audit reviewed 51 personnel files and determined that 3 of 51 have not complied. Department of Codes and Building Safety Management stated that due to the cyclical nature of the disclosure signing process, personnel hired after the cutoff date must wait for the subsequent round to sign the disclosures. Management, as a compensating control, had initiated its own new hire acknowledgement form. This was an all inclusive form that delineates specific certification and licensure requirements, and a supplementary conflict of interest statement. The conflict of interest clause specifically states that inspectors will not have any financial interests, in materials or labor, for any construction work while employed as an inspector for the Department.

Additionally, analytical procedures on contractor information contained within the KIVA system were performed. The analytical techniques involved matching 1,365 licensed contractors to the 87 employees within the Department of Codes and Building Safety to ascertain if matching addresses could be found. Results of the analysis indicated no matches between the files. We attempted to obtain trade inspection complaint records but were unable to secure them because there was no definitive customer complaint tracking procedure for trade inspections. The Building Inspection Chief handles complaints on an ad hoc basis and there was no transparency as to the determination of each call (See Observation E.)

2. *Does the Department of Codes and Building Safety ensure that inspectors are fully qualified to discharge their duties and protect public safety?*

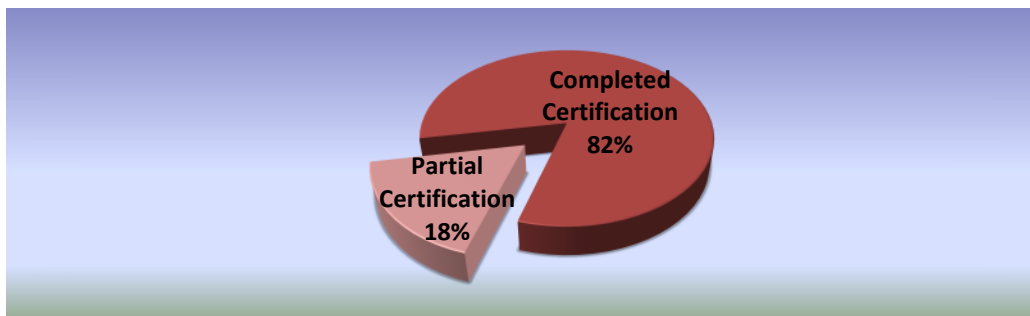
Yes. Procedures were in place designed to ensure inspectors were qualified to discharge their duties. To that end, the Office of Internal Audit evaluated policies, hiring practices, experience and qualifying license/certification requirements of the Department. There were 51 inspectors (including inspection chiefs) within the Department of Codes and Building Safety. Our evaluations indicated the following conditions:

- Hiring process followed all Metro Civil Service Rules.
- Candidates were reviewed and ranked by Human Resources as to qualifications, skills, education, and experience.
- Management conducts its own vetting process during screening of potential inspectors.

- Inspectors were required to acquire certifications within a set time period after getting hired; failure to do so can be grounds for termination.
- Actively licensed inspectors were required to maintain their licenses by following State (or Metro) mandated continuing professional education requirements; failure to maintain a license can be grounds for termination.
- All inspectors were required to sign Metro's annual financial and conflict of interest disclosure forms.

Additionally, we conducted reviews on the personnel files of 51 inspectors to determine the total number of inspectors that comply with certification/licensure requirements, as delineated in their job duties. We noted that most inspectors were required to obtain multiple certificates and/or licenses depending on job title. Exhibit C below describes that 42 (82%) of 51 inspectors have met complete certificate/licensure requirements and the remaining nine inspectors have partially complied or in the process of completing all needed certifications.

### Exhibit C - Inspector Certification Requirements



The average trade experience of all inspectors was over 12 years with tenure in the Department ranging from one year to 36 years. Procedures were in place to ensure that inspectors are qualified to discharge their duties.

3. *Does the Department of Codes and Building Safety have procedures in place to ensure the validity and completeness of reviews prior to issuance of a building permit?*

Yes. The permit tracking process is a step-wise procedure that begins with the permit application and ends with the Department's issuance of a building permit. The Office of Internal Audit noted that upon receipt of an application, a Zoning Examiner reviews the application, and the site plan, for compliance with the Metro Zoning Code. Depending on the size and scope of the project, the Zoning Examiner will also review other items such as contractor licensing credentials and other pertinent matters. The Zoning Examiner will also determine and assign the application to other departments and agencies for review and approval prior to issuance of the building permit. A printout of the agencies and sign-offs needed is prepared and presented to each applicant as a guide through the permit process.

To evaluate the effectiveness of the process we obtained a file of all 72,884 permits issued within the KIVA system. From this population, a sample of 90 transactions was randomly selected for review. The goal of the test was to ascertain completeness of review and sign-offs prior to issuance of the permit. Test results indicated that 89 (99%) of 90 permits issued had a well defined review and sign-off history. The test detected one transaction with an undeterminable review history; follow-up procedures indicated this was an appeal permit, related to a parent building permit, and was therefore not considered an exception. Procedures were in place to ensure reviews were complete prior to the issuance of a building permit.

4. *Does the Department of Codes and Building Safety have procedures in place to ensure the completeness of inspections prior to the issuance of a Use and Occupancy Certificate?*

Yes. According to the Metropolitan Code of Law, Chapter 16.36 Certificates of Occupancy, a Use and Occupancy certificate will be issued once the following has generally occurred:

- An application/request for a Use and Occupancy Certificate is received from a contractor or property owner
- Building inspections have been finalized
- Plumbing inspections have been finalized
- Electrical inspections have been finalized
- Gas/Mechanical inspections have been finalized
- Sewer has signed-off
- Water Services has signed-off

Depending on the type of construction (residential or commercial) and whether the construction is new or a remodel, certain inspections may or may not be required. Once it is established that all necessary inspections have been finalized, a Use and Occupancy certificate will be issued to the requesting party.

To evaluate the effectiveness of the process we obtained a listing of all Use and Occupancy transactions (applications and issued permits) between July 1, 2006 and March 31, 2009. From a population of 10,708 certificate transactions, we selected 130 random transactions for test work. The 130 transactions comprised of 73 residential, 27 commercial and 30 other assorted types (remodels, electrical, etc) of Use and Occupancy applications. Based on results of the tests, 107 Use and Occupancy certificates were issued and had the required inspections finalized prior to issuance of the certificate. The 23 applications not issued a certificate, were pending or denied with one or more incomplete final inspections and were not granted a certificate. Procedures were in place to ensure that inspections were complete prior to issuance of a Use and Occupancy Certificate.

5. *Are customer complaints for trade and property standards inspections handled in a timely manner?*

Generally yes. The Office of Internal Audit evaluated the timeliness of customer response by first obtaining a listing of all logged calls within the KIVA system for both Trade and Property Standards inspections. We previously noted that the current method for logging complaints for trade inspections was internal only to the Chief Building Inspector (see Observation E.) The Property Standards Division had logged calls they receive.

The Office of Internal Audit extracted Property Standards Division calls received between March 1, 2008 and March 31, 2009 resulting in 14,465 calls; 12,997 of which were resolved and 1,468 were open or pending. Evaluation of the listing proceeded by calculating the turnaround time for each call received using the difference between the date the calls were received and the initial inspection date.

Results of the evaluation indicated the following results:

- Average turnaround time was 13.8 days
- 7,049 (49%) call responses were initiated within 24 hours
- 12,921(89%) call responses were within 30 days
- 1,316 (9%) call responses were between 30 and 180 days
- 226 (1.5%) call responses were in excess of 180 days
- 2 calls appeared erroneously recorded because they showed negative turnaround times

Further review of calls responded to after 180 days revealed that KIVA was not consistently recording correct turnaround times. KIVA was allowing the input of two initial inspection dates that resulted in Department turnaround time summary reports being unverifiable (see Observation D.)

6. *Are Department expenditures reasonable, used for a valid Metro service delivery purpose, supported by documentation, and approved?*

Yes. In evaluating Department expenditures the Office of Internal Audit compared budgeted to actual expenditures and noted items that materially differ from the expected budget line items. A sample of significant line items were vouched to the transaction details to ascertain whether the expenditure items represented had the necessary supporting documentation; was appropriately approved and was used for a valid Metro service delivery purpose. We vouched a total of 51 transactions totaling \$145,311. Expenditures had the proper support, approval, and represented valid Metro service delivery purposes.

7. *Is the KIVA system protected from accidental and/or intentional damage to system assets?*

Generally yes. The Office of Internal Audit reviewed the Department's general security, regulatory compliance and business continuity procedures. We noted that although current procedures were functioning, there were areas where improvements could be made to enhance information systems security

practices and minimize the risk of accidental or intentional damage to system assets (see Observation C.)

8. *Does the Department of Codes and Building Safety have controls in place to ensure revenues are correct and complete and KIVA transactions reconcile with EnterpriseOne accounting information?*

Yes. We reviewed key control procedures for the cash receipts process, revenue recognition, and the reconciliation of information between separate computer systems. We obtained transaction reports from KIVA representing revenues from permitting activities. A sample of 119 transactions totaling \$6,820 was traced to the daily deposit slips and the general ledger posting in EnterpriseOne without any exceptions noted.

9. *Does the KIVA application have the necessary application controls in place to prevent misallocation of revenues?*

Generally yes. The Office of Internal Audit reviewed the Department's general security, regulatory compliance and business continuity procedures. We noted that although current procedures were functioning, there were areas where improvements can be made to enhance information systems security practices and minimize the risk of accidental or intentional damage to system assets (see Observation D.)

## **OBSERVATIONS AND RECOMMENDATIONS**

### **A – Determine Compliance Requirements for Payment Card Industry Data Security Standards**

The Department of Codes and Building Safety is one of the Metro Government's largest operations that accept credit card payments. Payment Card Industry Data Security Standards (PCI DSS) state compliance is mandatory for all merchants who accept, process, and/or transmit credit card information; even when those merchants contract the credit card processing function to third parties. The Department of Codes and Building Safety uses both Link2gov and Elavon as its credit card processors. While those contractors have provided evidence that they meet PCI DSS compliance requirements; the Department of Codes and Building Safety Management was not completely aware of the standards and was unable to identify the Department's responsibility related to PCI DSS requirements.

*Criteria:*

Payment Card Industry Data Security Standard

*Risk:*

Non-compliance to PCI DSS may hinder the ability of the Department to process fee payments therefore disrupting the normal flow of business. Additionally, non-compliance with PCI DSS standards may carry monetary penalties that may be substantial depending on which major credit card network levies the fines. Furthermore, non-compliant merchants can be barred from processing credit card transactions, assessed higher processing fees, and, in the event of a serious security breach, could be levied fines of up to \$500,000.

*Recommendation:*

Department of Codes and Building Safety Management should obtain an understanding of PCI DSS requirements and coordinate with other relevant departments such as Treasury and Information Technology Services Departments to ensure compliance with these requirements.

### **B – Initiate a Well Defined Service Level Agreement with Information Technology Services**

There were no policies, formal procedures, or well-defined service level agreements established with the Information Technology Services Department to systematically review issues and monitor performance of the KIVA application in accordance to the Department of Codes and Building Safety's business requirements.

*Criteria:*

International Organization of Standards Information Technology Security Standards (ISO 27002) Sections 6.1 and 10.2

*Risk:*

- Lack of general controls in KIVA application
- Lack of proper application performance monitoring
- Lack of inclusion into the Department's business continuity plan
- Insufficient of input/output validation controls

*Recommendation:*

The Department of Codes and Building Safety Management should establish a written service level agreement with the Information Technology Services Department. Having a written document that delineates and enumerates business requirements and expectations for information technology services will help ensure and monitor KIVA performance. The agreement should outline the Department's key business requirements that rely on services provided (such as: user account updates, input/output validation, change management, data backup, recovery plan and tests, etc.) The agreement should also define, and establish, a proper level of service that will enable the Department of Codes and Building Safety Management to monitor the performance of the KIVA application thereby ensuring reasonable business continuity.

## **C – Conduct a Thorough Computer/Information Systems Security Risk Assessment**

Information systems security practices should be enhanced to create a more secure information technology environment. The following observations were noted:

- The KIVA production environment was used for testing.
- The computing facility was not adequately protected from fire hazard due to its temporary nature.
- The Department's Business Continuity Plan did not include the impact of interruptions to the key business application (Accela/ KIVA.)
- The Business continuity plan was not distributed to the entire Department to ensure awareness.
- Although the KIVA application and database were fully backed up on a weekly schedule, we noted that incremental backups were not performed by Metro Information Technology Services on scheduled week days, as defined by the procedure.

*Criteria:*

International Organization of Standards Information Technology Security Standards (ISO 27002) Sections 7.1.1, 7.1.2, 9.2.1, 10.1.4, 10.5, 14.1, 14.1.4, and 14.1.5

*Risk:*

The following risks were identified in relation to information security practices:

- Interruption of normal business operation.

- Inaccurate data for managerial reporting.
- The business continuity plan may not be activated in time and/or may not be executed effectively.
- Backup data may not be accurate or usable when restore is needed for business continuity.
- The risk for inadequate physical protection includes application/data loss and interruption of business operations.

*Recommendation:*

Department of Codes and Building Safety Management should ensure a more robust information security environment by:

1. Establishing policies to limit non-business activities (development and testing) within the KIVA production environment.
2. Conducting a business impact analysis to understand the criticality of KIVA within the context of its operation. Performing the analysis would help define the requirements for KIVA data backup and restore testing.
3. Actively being involved in the KIVA application restores testing process to ensure that critical data and processes are reinstated accurately and correctly.
4. Initiating periodic requests for testing backup data to obtain reasonable assurance that operation can be recovered within the defined required time objective.

## ***D – Enhance the Computer System Monitoring Procedures***

There were no formalized review procedures conducted for the KIVA application. During our assessment of the Department of Codes and Building Safety’s information systems control practices, the Office of Internal Audit noted the following processes that should be enhanced concerning access controls, system monitoring, segregation of the test and production environment, and input validation procedures.

- Current user access control was insufficient to ensure all accounts for terminated employees were disabled or removed.
- Network groups and test user accounts associated with the KIVA application were found in the “Nashville” domain without a defined purpose.
- Generic KIVA management user accounts existed with high privileges.
- KIVA user accounts were not reviewed in accordance to job functions and updated promptly.
- Information Technology Services Department users and vendors had active accounts in production with elevated rights and privileges.
- Logging events for system activities and operational activities was not well defined.
- No formal or predefined log review process.
- Input validation errors.

*Criteria:*

International Organization of Standards Information Technology Security Standards (ISO 27002) Sections 10.2 and 10.10

*Risk:*

- User accounts not promptly updated may cause intentional and/or unintentional damage to data integrity.
- Uncontrolled user accounts can be intentionally or unintentionally used for malicious reasons.
- Weak fraud control when non-permitting clerks have access to forms and have subsequent permitting rights.

*Recommendation:*

Department of Codes and Building Safety Management should conduct a thorough application review of the KIVA system. The review should focus on ensuring that:

1. KIVA forms are classified based on sensitivity and criticality to the business operations.
2. Personnel have rights and privileges commensurate with their job function.
3. Vendor accounts are temporary and have rights and privileges commensurate with the business activity performed.
4. System logs and log monitoring requirements are well defined.
5. Input validation routines are correct.

## ***E – Improve the Customer Complaint Tracking Process***

Customer complaint tracking for Trade Inspections was not entered into the KIVA system. Trade Inspection complaints were handled by the Building Inspection Chief only. The files were kept in his office and not recorded within the KIVA system. The process was primarily internal to the Building Inspection Chief and was not transparent enough to provide adequate tracking of the cases from inception to resolution.

*Criteria:*

Prudent business practice

*Risk:*

- Lack of transparency for ascertaining customer service response from the initial complaint to the final resolution
- Inefficient recordkeeping

*Recommendation:*

Department of Codes and Building Safety Management should request a new permit "code" be added to KIVA that would allow customer complaint tracking for Trade Inspections. Adding a new code would establish transparency for

the process, enable efficient response to the complaints, and provide a medium for measuring performance as they pertain to customer service.

# GENERAL AUDIT INFORMATION

## STATEMENT OF COMPLIANCE WITH GAGAS

We conducted this performance audit from March 2009 to July 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives. Our audit included tests of management controls that we considered necessary under the circumstances.

## SCOPE AND METHODOLOGY

The audit period focused primarily on the period July 1, 2006 through March 31, 2009 financial balances, transactions, and performance on the processes in place during the time of the audit.

The methodology employed throughout this audit was one of objectively reviewing various forms of documentation, including written policies and procedures, financial information, various forms of data, reports and information pertaining to the Department of Codes and . Additionally, management, administrative and operational personnel were interviewed and directly observed.

## CRITERIA

In conducting this audit, the existing Department of Codes and Building Safety processes were evaluated for compliance with:

- *The Committee of Sponsoring Organizations Internal Control-Integrated Framework*
- *International Organization of Standards Information Technology Security Standards (ISO 27002)*
- The Code of the Metropolitan Government of Nashville and Davidson County
- Metropolitan Code of Law, Chapter 16.36 Certificates of Occupancy
- Metro Finance Treasury Policy #9, Cash Deposits
- Standards promulgated by the International Code Council
- Prudent Business Practices

## STAFF ACKNOWLEDGEMENT

Carlos Holt, CPA, CIA, CFE, CGAP - Audit Manager  
Mel Marcella, CPA, CIA, CFE – In Charge Auditor  
Tracy Carter – Staff Auditor  
Qian Yuan – Staff Auditor

## **APPENDIX A. MANAGEMENT RESPONSE**

- Management's Responses Starts on Next Page -

KARL F. DEAN  
MAYOR



**METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

DEPARTMENT OF CODES & BUILDING SAFETY

September 24, 2009

OFFICE ADDRESS  
METRO OFFICE BUILDING – 3rd FLOOR  
800 SECOND AVENUE, SOUTH  
NASHVILLE, TENNESSEE 37210

MAILING ADDRESS  
POST OFFICE BOX 196300  
NASHVILLE, TENNESSEE 37219-6300  
TELEPHONE (615) 862-6500  
FACSIMILE (615) 862-6514  
[www.nashville.gov/codes](http://www.nashville.gov/codes)

Mr. Mark Swann  
Metropolitan Auditor  
Office of Internal Audit  
222 3<sup>rd</sup> Avenue, North, Suite 401  
Nashville, TN 37201

Re: Department of Codes & Building Safety

Dear Mr. Swann:

This letter acknowledges that the Metropolitan Department of Codes and Building Safety received the report entitled; Audit of the Department of Codes and Building Safety. The department has evaluated all of the audit recommendations raised in the report. Each audit recommendation and suggested action plan for correction has been considered. Whenever possible, changes have or will soon be implemented. Specific concerns that may impede implementation of some recommendations are expressed in the attached response.

The Department of Codes and Building safety would like to express its appreciation for your assistance and cooperation during this process. Any improvement that this department can make toward increasing the efficiency of the Metropolitan Government is always welcomed.

Sincerely,

A handwritten signature in black ink, appearing to read 'T. Cobb', with a long horizontal flourish extending to the right.

Terrence L. Cobb  
Director

BUILDING • ELECTRICAL • GAS/MECHANICAL • PLUMBING • PROPERTY STANDARDS • ZONING

**Department of Codes and Building Safety Management Response to Audit Recommendations  
September 2009**

Report Item and Description	Response to Recommendation / Action Plan	Assigned Responsibility	Estimated Completion
<p><b>A.</b> Department of Codes and Building Safety Management should obtain an understanding of PCI DSS requirements and coordinate with other relevant departments such as Treasury and Information Technology Services Departments to ensure compliance with these requirements.</p>	<p><b>Agree.</b> The Department acknowledges the validity of this recommendation and will undertake the process of coordinating with other departments (Legal, Treasury, ITS) to implement whatever controls necessary to comply with PCI requirements. Once again, the Department was without the necessary expertise and/or knowledgeable personnel to understand the ramifications of the PCI requirements necessary to process fee payments. The Department will take ownership of our share of these PCI requirements and will begin the process of implementing controls to reduce any potential problems by working with other relevant Metro departments.</p>	<p>Roy Jones, Carla Langley</p>	<p>September 1, 2010</p>
<p><b>B.</b> The Department of Codes and Building Safety Management should establish a written service level agreement with the Information Technology Services Department. Having a written document that delineates and enumerates business requirements and expectations for information technology services will help ensure and monitor KIVA performance. The agreement should outline the Department's key business requirements that rely on services provided (such as: user account updates, input/output validation, change management, data backup, recovery plan and tests, etc.) The agreement should also define, and establish, a proper level of service that will enable the Department of Codes and Building Safety Management to monitor the performance of the KIVA application thereby ensuring reasonable business continuity</p>	<p><b>Agree.</b> The Department will begin the process of establishing a written SLA with Metro ITS. As noted in Metro's Internal Audit recommendation, we will outline through the SLA our business expectations of ITS as they relate to the KIVA system. Once established, the Department will monitor the SLA for compliance.</p>	<p>Roy Jones, Joey Hargis</p>	<p>June 30, 2010</p>
<p><b>C.</b> Department of Codes and Building Safety Management should ensure a more robust information security environment by:</p> <ol style="list-style-type: none"> <li>1. Establishing policies to limit non-business activities (development and testing) within the</li> </ol>	<p><b>Agree.</b> The Department believes the recommendations as state are valid and will initiate with Metro ITS the following actions:</p> <ul style="list-style-type: none"> <li>• Establish policies to limit non-business activities with the KIVA production environment.</li> <li>• Work to establish procedures to monitor and</li> </ul>	<p>Roy Jones, Joey Hargis</p>	<p>June 30, 2010</p>

**Department of Codes and Building Safety Management Response to Audit Recommendations  
August 2009**

Report Item and Description	Response to Recommendation / Action Plan	Assigned Responsibility	Estimated Completion
<p>KIVA production environment.</p> <ol style="list-style-type: none"> <li>2. Conducting a business impact analysis to understand the criticality of KIVA within the context of its operation. Performing the analysis would help define the requirements for KIVA data backup and restore testing.</li> <li>3. Actively being involved in the KIVA application restores testing process to ensure that critical data and processes are reinstated accurately and correctly.</li> <li>4. Initiating periodic requests for testing backup data to obtain reasonable assurance that operation can be recovered within the defined required time objective.</li> </ol>	<p>review system logs.</p> <ul style="list-style-type: none"> <li>• Conduct a business impact analysis related to the proper and timely backup procedures for the KIVA system.</li> <li>• Appoint an appropriate member of Codes' management to monitor the backup testing process for Codes' critical data.</li> <li>• Work closely with other Metro personnel on keeping its Business Continuity &amp; Disaster Recovery plan current. In the past every incident where the department has had to implement any type of data recovery and/or shift into "disaster mode", the department has been able to do so effortlessly. However, we do recognize that continuing testing and updating of our Business Continuity Plan is crucial. With that in mind, the Department will conduct a business impact analysis of its plan in conjunction with knowledgeable Metro personnel familiar with this process taking care to specifically address application/data recovery for our KIVA application.</li> <li>• Establish a procedure to ensure that periodic backups are being performed by Metro ITS.</li> </ul>		
<p><b>D.</b> Department of Codes and Building Safety Management should conduct a thorough application review of the KIVA system. The review should focus on ensuring that:</p> <ol style="list-style-type: none"> <li>1. KIVA forms are classified based on sensitivity and criticality to the business operations.</li> <li>2. Personnel have rights and privileges commensurate with their job function.</li> <li>3. Vendor accounts are temporary and have rights and privileges commensurate with the business activity performed.</li> <li>4. System logs and log monitoring requirements are well defined.</li> <li>5. Input validation routines are correct.</li> </ol>	<p><b>Agree.</b> The Department recognizes the department is responsible for the "ownership" of all information generated through the KIVA system. That being said, however, the Department relies heavily upon Metro's ITS Department to help maintain and serve the KIVA system due to the fact that Codes does not have the expertise and/or knowledgeable personnel to do so. The Department will work in conjunction with Metro ITS to bring all recommendations stated in this finding (assigning access rights according to job functions, review access to appropriate <i>fgroups</i>, restricting vendor rights to KIVA information, etc.) into compliance with best practices as detailed by the recommendation</p>	<p>Roy Jones, Joey Hargis</p>	<p>June 30, 2010</p>

**Department of Codes and Building Safety Management Response to Audit Recommendations  
August 2009**

Report Item and Description	Response to Recommendation / Action Plan	Assigned Responsibility	Estimated Completion
	<ul style="list-style-type: none"> <li>• The Department will also review its formal termination process, commit it to writing, and establish the process in coordination with the ITS Department.</li> <li>• The Department agrees with the recommendation and will work with Metro ITS to classify our KIVA system and operational activities.</li> <li>• The KIVA system has been on-line for approximately three (3) years. During those three years there has been a constant refining of system procedures and protocols; new programs have been brought on-line every few months or so. Departmental reports have been, and still are, in the process of being produced and refined as the department's needs have changed. Each new system upgrade has brought increased improvement in the accuracy of system-generated reports. The Department is aware of the issues concerning unverifiable turn-around times in our Property Standards division reports and has been working with ITS to resolve this reporting deficiency. The Department will continue to work with Metro ITS to refine input valuation data in order to eliminate multiple initial inspection dates so that more accurate and verifiable turn-around times are generated.</li> </ul>		
<p><b>E.</b> Department of Codes and Building Safety Management should request a new permit "code" be added to KIVA that would allow customer complaint tracking for Trade Inspections. Adding a new code would establish transparency for the process, enable efficient response to the complaints, and provide a medium for measuring performance as they pertain to customer service.</p>	<p><b>Agree.</b> The Department acknowledges the validity of this recommendation and will work with Metro ITS to establish a new permit code which will allow customer complaint tracking for trade inspections.</p>	<p>Roy Jones, Joey Hargis</p>	<p>June 30, 2010</p>