Performance Audit:
Information Technology
General Controls

November 2010

City Auditor's Office

City of Atlanta

File #09.06

CITY OF ATLANTA
City Auditor's Office
Leslie Ward, City Auditor
404.330.6452

November 2010

Performance Audit:

Information Technology General Controls

Why We Did This Audit

We undertook this audit because prior audits identified problems with specific information system applications. The city's chief information officer also expressed concerns about inadequate staffing, risks to network security, and lack of disaster recovery and business continuity plans.

What We Recommended

The chief information officer should:

- update department policies to strengthen security and to reflect actual practices
- update the department's strategic plan to reflect the city's current needs
- work with departments to establish service level agreements consistent with the department's updated strategic plan
- evaluate options and seek funding to develop business continuity and disaster recovery plans for the city
- ensure that approval for system changes is documented prior to implementation
- work with the city attorney to identify laws and regulations that affect city data
- work with the Department of Finance to establish a process to reconcile differences between Kronos and Oracle
- work with the Department of Human Resources to ensure the department is notified when employees leave city employment

For more information regarding this report, please contact Eric Palmer at 404.330.6455 or epalmer@atlantaga.gov.

What We Found

The Department of Information Technology has implemented sufficient controls in 59% of the areas we evaluated, but significant risks remain. We analyzed the department's general controls for 20 of 34 business processes covered by the COBIT framework. We identified areas where policies were inadequate to meet the intent of COBIT or did not match practices. The department lacks disaster recovery and business continuity plans, procedures to monitor security logs, assessment of legal and regulatory requirements and service agreements with other departments. The city has a sound change management policy but technical documents were incomplete for a randomly selected change to the Oracle system. While some processes to manage user accounts are strong, the department does not enforce the city's guidelines for strong passwords in Oracle and more than 200 employees who no longer work for the city retained access to Oracle and the network. We noted similar issues for aviation and watershed applications in previous reports.

The department estimated it needed an additional 85 staff — more than double its current level — in a December 2009 presentation prepared for the new administration and City Council. While we agree that the department appears to be understaffed, omissions and errors in the analysis overstated staffing needs in some areas and understated staffing needs in others. Although the presentation purported to use industry standards to identify staffing needs, more than half of calculations were based on staff's professional judgment and some data used in calculations lack support. We estimate that the department needs an additional 49 staff members based on industry standards and data that we could verify.

We also followed up on the department's progress implementing open audit recommendations and found that 11 of the 16 recommendations that we assessed have been implemented. While the department developed a report to identify potential payroll errors as we recommended, the report we reviewed was incomplete, resulting in undetected errors.

Management Responses to Audit Recommendations

Summary of Management Responses

Recommendation #1:	The chief information officer should update department policies to strengthen security and to reflect actual practices.	
Response & Proposed Action:	The CIO has revised procedures to address backup, restore, and operating system security logs. DIT is working with human resources to strengthen policies for removing user access. DIT will be changing the Oracle password policies.	**Agree**
Timeframe:	Oracle password policy change will be in mid-November.	
Recommendation #2:	The chief information officer should update the department's strategic plan to reflect the city's current needs.	
Response & Proposed Action:	The CIO has developed a three-year strategic plan that reflects the Mayor's strategic focus areas and budget needs.	**Agree**
Timeframe:	Complete	
Recommendation #3:	The chief information officer should work with departments to establish service level agreements consistent with the department's updated strategic plan.	
Response & Proposed Action:	The strategic plan consolidates the IT groups from watershed and aviation with DIT and establishes service level agreements with the departments.	**Agree**
Timeframe:	TBD dependent upon the IT consolidation initiative	
Recommendation #4:	The chief information officer should evaluate options and seek funding to develop business continuity and disaster recovery plans for the city.	
Response & Proposed Action:	The CIO is developing a disaster recovery RFP. Additional funding and a business continuity champion are needed for the disaster recovery plan to be effective.	**Agree**
Timeframe:	TBD	
Recommendation #5:	The chief information officer should ensure that approval for system changes is documented prior to implementation.	
Response & Proposed Action:	Essential support staff will provide approval at weekly change management calls. Database administrators will review documentation before production.	**Agree**
Timeframe:	Complete	
Recommendation #6:	The chief information officer should work with the city attorney to identify laws and regulations that apply to city data and develop procedures to classify and protect data commensurate with requirements.	
Response & Proposed Action:	The Department of Law is researching the laws and regulations. DIT will work with the Department of Law to develop procedures.	**Agree**
Timeframe:	TBD	
Recommendation #7:	The chief information officer should work with the controller to establish a process to reconcile differences between Kronos and oracle.	
Response & Proposed Action:	The CIO will work with the controller to establish a process.	**Agree**
Timeframe:	Dependent on controller's availability and priority.	
Recommendation #8:	The chief information officer should work with the commissioner of human resources to ensure the department is notified when employees leave city employment to enable prompt removal of user access to city systems.	
Response & Proposed Action:	We are working with human resources to strengthen policies.	**Agree**
Timeframe:	Dependent on human resources commissioner's availability and priority.	

CITY OF ATLANTA

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
(404) 330-6452
FAX: (404) 658-6077

LESLIE WARD
City Auditor
lward1@atlantaga.gov

AMANDA NOBLE
Deputy City Auditor
anoble@atlantaga.gov

AUDIT COMMITTEE
Fred Williams, CPA, Chair
Donald T. Penovi, CPA, Vice Chair
Marion Cameron, CPA
C.O. Hollis, Jr., CPA, CIA
Ex-Officio: Mayor Kasim Reed

November 2, 2010

Honorable Mayor and Members of the City Council:

We initiated this audit because prior audits identified problems with specific information system applications. The city's chief information officer also expressed concerns about inadequate staffing, risks to network security, and a lack of disaster recovery and business continuity plans. We focused our tests of controls on the network, the operating system for Oracle, and the city's two enterprise-wide systems: Oracle and Kronos. We reviewed the department's general controls for 20 of the business processes covered under the COBIT (Controls Objectives for Information and related Technology) framework. We also followed up on the department's progress implementing audit recommendations open as of July 2009.

Our recommendations focus on reducing the risks we identified. We recommended that the department update its security policies and strategic plan, work with departments to establish service level agreements, evaluate options and seek funding to develop disaster recovery and business continuity plans, and ensure that approval for system changes is documented prior to implementation. We also recommended that the chief information officer work with the city attorney to identify laws and regulations that affect city data, work with the Department of Finance to establish a process that reconciles differences between Oracle and Kronos, and work with the Department of Human Resources to ensure that the Department of Information Technology is notified when employees leave city employment. Management agrees with our recommendations. Their full responses to our recommendations are appended to the report.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We appreciate the courtesy and cooperation of city staff throughout the audit. The audit team for this project was Damien Berahzer, Katrina Clowers and Eric Palmer.

Leslie Ward
City Auditor

Fred Williams
Fred Williams
Audit Committee Chair

Information Technology General Controls

Table of Contents

Introduction 1

Background 3

Previous Audits Identified Information Technology Control Weaknesses 5

Audit Objectives 7

Scope and Methodology 7

Findings and Analysis 11

Stronger Controls Needed to Protect Critical Systems 11

Implemented Controls Reduce Several Risks 11

Some Practices Reduce Risk but Should Be Documented 14

Staff Did Not Follow Some Policies that Would Reduce Risk 15

No Policy or Practice for Over One-Fourth of Needed Controls 17

Department Appears Understaffed but Staffing Plan Overstates Need 19

The Plan Overstates Needs in Some Areas and Understates Need in Others 20

The Department Has Made Progress Implementing Recommendations 23

The Department Has Implemented Most Recommendations 23

Timekeeping Continues to Pose Risk 25

Recommendations 27

Appendices 29

Appendix A Management Review and Response to Audit Recommendations 31

Appendix B Implementation of Audit Recommendations by Risk Category 37

List of Exhibits

Exhibit 1 Department of Information Technology Organizational Chart 4

Exhibit 2 Information Technology Budgets Fiscal Year 2010 4

Exhibit 3 IT Policies and Practices Compared to COBIT 12

Exhibit 4 Recalculation of Staffing Need 22

Exhibit 5 Implementation Status by Risk Area 24

Introduction

We conducted this performance audit of the Department of Information Technology's general controls pursuant to Chapter 6 of the Atlanta City Charter, which establishes the City of Atlanta Audit Committee and the City Auditor's Office and outlines their primary duties. The Audit Committee reviewed our audit scope in March 2010.

A performance audit is an objective analysis of sufficient, appropriate evidence to assess the performance of an organization, program, activity, or function. Performance audits provide assurance or conclusions to help management and those charged with governance improve program performance and operations, reduce costs, facilitate decision-making and contribute to public accountability. Performance audits encompass a wide variety of objectives, including those related to assessing program effectiveness and results; economy and efficiency; internal controls; compliance with legal or other requirements; and objectives related to providing prospective analyses, guidance, or summary information.[1]

We undertook this audit because prior audits related to specific information system applications identified problems. The city's chief information officer also expressed concerns about inadequate staffing, risks to network security, and lack of disaster recovery and business continuity plans.

Our audit focuses on the Department of Information Technology's general controls using the COBIT (Control Objectives for Information and related Technology) framework. General controls relate to access, security, disaster recovery, change management, and documentation requirements that cut across information technology applications and systems. COBIT is a set of generally accepted best practices related to information technology that covers 34 business processes grouped into four broad areas:[2]

[1] Comptroller General of the United States, *Government Auditing Standards,* Washington, DC: U.S. Government Accountability Office, 2007, p. 17-18.

[2] IT Governance Institute, *IT Assurance Guide Using COBIT*, 2007, p. 25.

- **Plan and Organize** – development of an organization's overall technology strategy, management and investment to meet strategic goals
- **Acquire and Implement** – identification of requirements, acquiring and implementing the technology, and developing a maintenance plan
- **Deliver and Support** – operation of applications and support including security and training
- **Monitor and Evaluate** – assessment of whether the current system meets the designed objectives and if controls are sufficient to comply with regulatory requirements

We reviewed selected policies and controls for 20 of the 34 business processes covered in the COBIT framework. While we reviewed aspects of all four broad organizational areas covered in the framework, we focused most attention on service delivery and support.

We also followed up on the department's progress in implementing 23 audit recommendations open as of July 2009. The city auditor's office is responsible for assessing the implementation of prior audit recommendations and reporting on management's corrective actions and significant findings that management has not fully addressed. We made these recommendations in three reports issued in 2007 and 2008:

- *Police Computer Aided Dispatch Data Reliability,* April 2008
- *Review of the Oracle ERP First Payroll Run,* April 2008
- *ERP Implementation Assessment for the City of Atlanta,* June 2007 (conducted by KPMG LLP)

Based on our assessment, seven of the recommendations — all made in the 2007 ERP Implementation Assessment — are no longer relevant because they dealt with risks the city faced while transitioning to the new Oracle system. Most of the 16 recommendations we followed up on dealt with process improvements or strengthening controls to safeguard information assets. Appendix B shows detail of each recommendation and status by risk category. Management agreed with all of the recommendations.

Background

The Department of Information Technology's mission is to collaborate with other departments to facilitate cost-effective use of technology. The department supports the city's information technology infrastructure and an estimated 175 applications that other city departments use to provide services to the public or manage administrative functions. As of October 2009, the department had 111 positions (see Exhibit 1), including 30 contractors. The department is organized into nine units that provide the following services:

- Business Strategic Services focuses on program and project management best practices, strategy development, governance, and using existing technology.

- Telecommunications is responsible for the hardware, telephone infrastructure, and vendor management for citywide telecommunications.

- Network and Server Operations maintains the general fund servers, network equipment and inventory, data storage, and backup equipment.

- Data Center Operations provides continuous mainframe support for departments, prints large scale forms, handles file transfers, and processes checks. The Data Center acts as the help desk after normal business hours

- End User Support and Help Desk work to resolve technology issues for city users.

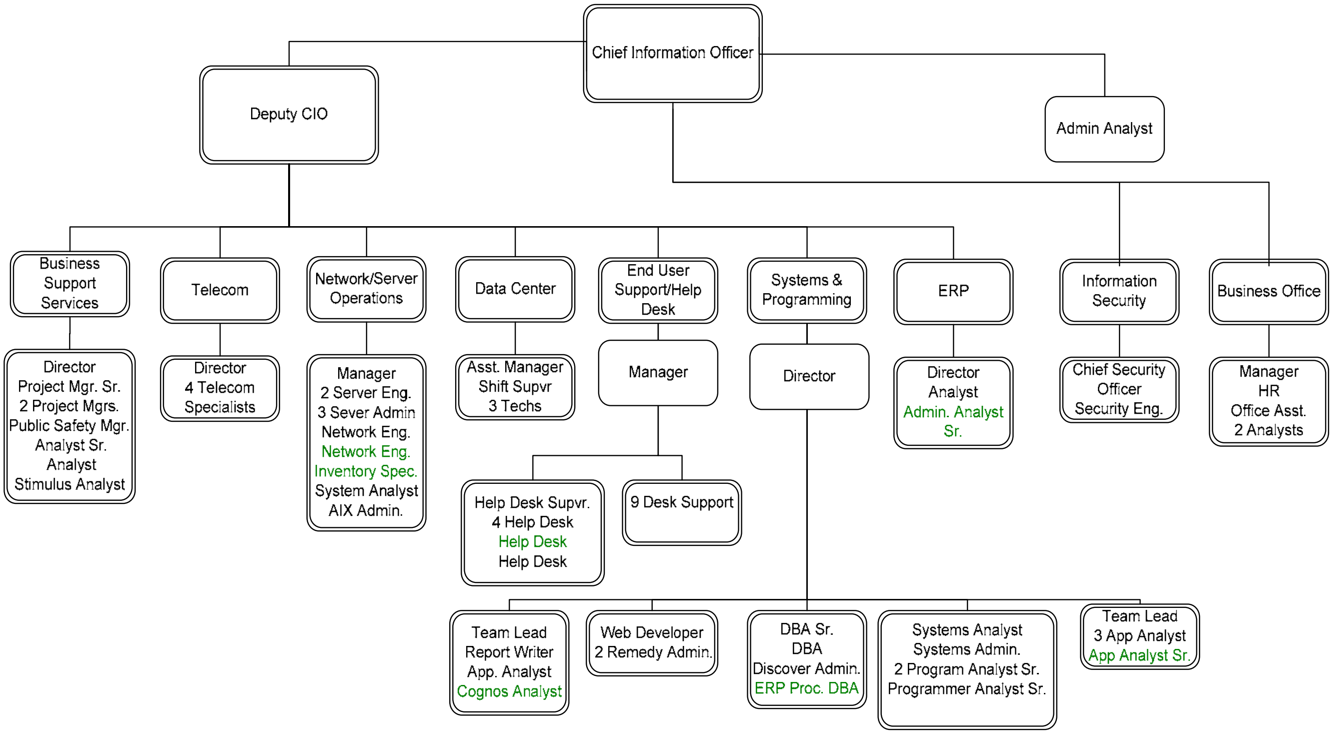
- Systems and Programming supports the city's applications and databases.

- Enterprise Resource Planning manages the city's Oracle system, which integrates procurement, finance, human resources, and payroll transactions.

- Information Security protects the city's computer data and information assets from security threats.

- Business Office provides departmental administrative support.

Exhibit 1 Department of Information Technology Organizational Chart



Source: Department of Information Technology, as of October 27, 2009

Note: Green text represents vacant positions

The city budgeted almost $55 million for information technology in fiscal year 2010, including the Department of Information Technology and information technology groups within the departments of Aviation and Watershed Management. About $19 million of the budget was for personnel and almost $16 million was for consultants (see Exhibit 2).

Exhibit 2 Information Technology Budgets Fiscal Year 2010

	Information Technology	Aviation	Watershed Management	TOTAL
Total IT Budget	$ 29,686,392	$ 10,997,367	$ 14,234,823	$ 54,918,582
Personnel	$ 6,422,553	$ 4,409,947	$ 8,124,638	$ 18,957,138
Consulting	$ 9,872,800	$ 2,491,713	$ 3,536,495	$ 15,901,008

Source: City of Atlanta's Oracle Financials application and FY 2010 IT budget detail as of April 2010

Previous Audits Identified Information Technology Control Weaknesses

Weak information technology controls increase the risk of inaccurate or lost data. Previous audits identified weaknesses in change management, lack of validation controls between the city's timekeeping and payroll systems, and inadequate procedures to remove system access from former employees. The city's financial auditor also noted control deficiencies in management letters accompanying the city's fiscal year 2008 and 2009 audited financial statements and recommended strengthening general information technology and application-specific controls.

Change management policies not followed. The Department of Information Technology did not follow its change management policy when attempting to fix a faulty interface between Oracle — the city's financial management system — and the Department of Aviation's invoicing system. We reported in our August 2009 performance audit, *Airport Terminal Leases,* that the Department of Information Technology agreed to reconfigure coding in the Oracle accounts receivable module to prevent problems affecting the posting of about one percent of aviation invoicing transactions. However, the department developed the proposed solution without involving Department of Finance functional staff or the ERP (Enterprise Resource Planning) steering committee, which is responsible for ensuring that the system meets the city's goals and objectives.

The change management policy calls for "owner departments," those directly responsible for data, to approve all changes before the Department of Information Technology proceeds with the change. When multiple departments own the data, as is the case in Oracle, all owner departments must approve the change. Failure to include key stakeholders in change decisions increases the risk that changes will introduce new problems that could destabilize a critical system. We recommended the Department of Information Technology involve key stakeholders and application owners early in the change management process in order to provide time for meaningful analysis of options and identify risk to the system to address future problems with the system.

We reported in our December 2009 performance audit, *Department of Watershed Management Customer Information System,* that watershed management stated that change management was the sole responsibility of the contractor that maintains its billing system. However, the city's maintenance agreement with the contractor identified portions of change management, including testing and approving changes before they are put into production, as the city's responsibility. Because watershed management misunderstood its change management responsibilities, neither city staff nor the contractor adequately tested a new program to calculate and apply back-billed water and sewer charges. Consequently, the Department of Watershed Management incorrectly applied late penalties to 40,000 accounts before catching and correcting the error.

Overtime errors not detected. The city miscalculated overtime for nearly 1,700 employees in its first payroll processed in Oracle. We reported in our April 2008 performance audit, *Review of the Oracle ERP First Payroll Run*, that the city overpaid about $243,000 in overtime due to improper data entries in the Kronos timekeeping system. The interface between Kronos and Oracle required department timekeepers to account for time more precisely than they had when Kronos was interfaced with PeopleSoft. Some timekeepers had developed a practice of entering all of an employee's overtime for a pay period into one entry rather than recording the actual hours worked per day, which resulted in overtime calculation errors in Oracle. Kronos technicians were unaware of the informal timekeeping practice and therefore didn't address it when testing the interface with Oracle or in training. We recommended the chief information officer develop automated or semi-automated controls to detect errors and validate timekeeping totals originating in Kronos.

Employees retained system access after leaving city employment. We identified accounts of former employees that were still active, which increases risk of unauthorized access or changes to sensitive data. We reported in the *Airport Terminal Leases* audit that 14 of 73 user accounts in the department's billing system belonged to former employees. Four of these accounts provided access to create, update, and delete both lease agreements and invoices. In the *Department of Watershed Management Customer Information System* audit, we identified three of a random sample of 25 user accounts as belonging to former employees. Failure to inactivate accounts provides opportunities for misuse of data or fraud. Watershed management removed access for accounts that we identified. We recommended the departments periodically review and recertify application users' level of access and remove terminated users.

External audits recommended additional controls. The city's financial auditor recommended strengthening information technology controls in management letters accompanying the city’s 2008 and 2009 audited financial statements. In 2009, the financial auditor recommended that the Department of Information Technology regularly rotate personnel, classify confidential data, and secure administrator manuals. In 2008, the financial auditor recommended that the department formalize its security testing process and save test results for at least 90 days. The financial auditor also made several recommendations to the watershed management technology group, including establishing a change control process, tracking employee transactions, using software to manage updates, and regular security monitoring. We followed up on the status of the external audit recommendations and will report later in November.

Audit Objectives

This report addresses the following objectives:

- Are controls in place to maintain data integrity and data security for critical city systems?
- Are the staffing needs identified in the Department of Information Technology’s November 2009 transition plan reasonable?
- To what extent has the department implemented previous audit recommendations?

Scope and Methodology

We conducted this audit in accordance with generally accepted government auditing standards. We focused our tests of controls on the network, the AIX operating system housing the Oracle application and the city’s two enterprise-wide systems: Oracle and Kronos. Failure in any of these systems could affect all city operations. Oracle and Kronos are the city’s only enterprise wide financial applications and the city’s network provides access to other citywide applications. We conducted our analysis of the network, Kronos, and Oracle from January through May 2010. Our analysis of former employees with user access covered all employees who left city employment beginning December 2008 through December 2009. We did not evaluate whether enterprise information technology functions should be consolidated under the Department of Information Technology.

Our audit methods included:

- reviewing Department of Information Technology policies to understand intended control procedures
- interviewing department personnel to understand how procedures are followed in practice
- walking through key controls to identify areas of high risk
- comparing department policies and practices to the COBIT framework
- analyzing access to Oracle, Kronos, the network, and restricted areas of city hall to determine whether any active IDs belonged to former city employees
- reviewing security settings for the Oracle operating platform
- reviewing the methods, calculations, and supporting data for the department's November 2009 staffing plan
- following up on the status of previous recommendations, including:
    - interviewing department management and staff to understand the status of the recommendations
    - reviewing change documentation
    - reviewing reports on contractor work
    - checking the validation process for 911 reporting
    - interviewing payroll to discuss the validation process
    - analyzing time entries in Oracle and Kronos for the pay period ending April 14, 2010

Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We provided the chief information officer a detailed description of the results of our AIX security assessment April 2010. This report summarizes the findings and recommendations related to security, but excludes details about specific vulnerabilities. Vulnerability assessments for technology infrastructure are not subject to disclosure under the Georgia Open Records Act.[3]

[3] O.C.G.A. § 50-18-72(15)(A)(i).

Findings and Analysis

Stronger Controls Needed to Protect Critical Systems

The Department of Information Technology has implemented sufficient controls in 59% of the areas we evaluated, but significant risks remain. Effective entity-wide controls help ensure the department is able to support the city's critical information technology infrastructure and applications such as Oracle and Kronos. Control weaknesses present risks to the city's ability to comply with data regulations, maintain data integrity, continue operations or recover from a disaster, provide needed services to the departments, and restore lost email.

Department policies and procedures protect against external attacks from viruses, worms, spyware, adware and Trojan horses. The department has also implemented controls that protect the physical environment where critical systems are housed. Its organizational structure aligns with key business areas and duties are segregated to reduce the possibility for a single individual to compromise a critical process. The department's use of state negotiated contracts provides opportunities for the city to save money on hardware and software purchases.

We also identified areas where policies were insufficient or did not match practices. The department lacks disaster recovery and business continuity plans, procedures to monitor security logs, assessment of legal and regulatory requirements and service agreements with other departments. The city has a sound change management policy but technical documents were incomplete for a randomly selected change to the Oracle system. While some processes to manage user accounts are strong, the department does not enforce the city's guidelines for strong passwords in Oracle and more than 200 employees who no longer work for the city retained access to Oracle and the network.

Implemented Controls Reduce Several Risks

The Department of Information Technology has implemented policies and practices to reduce the city's risk. The department established policies that govern the city's use of firewall and antivirus programs, implemented measures to protect technology assets, structured organizational units along business functions, developed procedures for granting and removing user access from systems, and has implemented tools and methods to manage vendors. The department also protects Oracle through limiting change authorization, segregating change duties, and testing changes with the system users.

Exhibit 3 summarizes the results of our assessment of department control policies and practices compared to the COBIT framework. In half of the control objectives we evaluated, the department's policies were consistent with COBIT and practices were consistent with the department's policies. In another 9% of the control objectives we evaluated, the department's practices were consistent with COBIT, but differed from policy or a policy is not yet established. We identified risks in 41% of the control objectives evaluated, where staff failed to follow or enforce existing policies (13%) or policies and practices are inadequate to meet the intent of COBIT.

Exhibit 3 IT Policies and Practices Compared to COBIT

	Policy and Practice OK	Policy Issue; Practice OK	Policy OK; Practice Issue	Policy and Practice Issues
Plan and Organize	4	1	3	1
Acquire and Implement	4	1	1	2
Deliver and Support	15	2	2	8
Monitor and Evaluate	0	0	0	2
Total Elements Covered	**23**	**4**	**6**	**13**
	50.00%	8.70%	13.04%	28.26%
	59%		41%	

Source: City Auditor's Office: Summary of audit fieldwork performed compared to the four COBIT domains

Controls reduce the risk that attacks will damage the city's network. The department has developed and implemented policies that govern the use of firewall and antivirus protection. A firewall is software or hardware that prevents hackers, viruses, and worms from gaining access to computer systems. Antivirus software prevents, detects, and removes malware (viruses, worms, spyware, adware, and Trojan horses). These systems work together as an initial defense against external threats by:

- specifying the types of data packets that can be transmitted through the network

- limiting the size of data packets transmitted at a time to prevent traffic overload
- verifying sender identity to prevent "spoofing"
- alerting the system administrator if the system is attacked
- generating reports on systems and computers with viruses

Controls physically protect city resources. The department protects the city's servers and network devices from sabotage, theft, and failure due to environmental changes. The city's main servers are stored behind locked doors that require electronic key card access for entry. Security cameras monitor access to the restricted areas. Servers in the restricted areas are mounted on racks standing on raised floors. The temperature of the rooms is regulated by cooling systems and department staff checks the temperature of the server rooms daily to protect against system overheating and malfunctions. In addition, the city has installed a dry pipe fire suppression system to reduce the loss from a fire and implemented an uninterruptable power source to continue operations during power outages.

Processes for adding new users protect system security. The department has established processes to confirm that user access to systems and data are in line with job requirements. Operating departments request system access for specific employees and their supervisors must approve the request. The Department of Information Technology logs all requests for access into the Remedy system. Technical staff responsible for the function for which access is requested reviews each request to ensure requested access to data and systems is commensurate with the employee's job. Two levels of review and approval reduce the risk that the employees will be granted inappropriate access to sensitive data or have the ability to perform incompatible duties within a system.

The department has controls to manage vendors. The department reduces vendor risks of overpricing and underperformance through its use of state contracts and contract management software. The department uses federal and state contracts to leverage government discounts for software. The department uses contract management software to record and track contract information and documents. The software also helps the department to supervise the contract and evaluate whether services are delivered in accordance with contract terms. The department supplements city staff with consultants to provide flexibility to adapt to changing needs and contractors help to train city technical staff.

The Department has controls to manage changes to the Oracle system. The department developed a process to govern how changes are made to Oracle. All changes are required to be documented on a change request form and tracked in the Remedy system. The form includes a description of the problem to be addressed, the functional team's assessment of the problem and recommended resolution, design requirements, if applicable, identification of alternatives, justification and cost benefit of the recommended resolution, time required, and risk. All proposed changes are to be discussed and approved by the change control committee prior to implementation. Any cost impact is submitted to the ERP steering committee for approval or denial. User acceptance testing is required before the change can be submitted for migration to the production environment.

Some Practices Reduce Risk but Should Be Documented

Although some of the department's control practices were not documented in policy or differed from the policies in place, the practices met the intent of the control objectives identified in the COBIT framework. The chief information officer should update department policies to reflect actual practices in order to clarify expectations of staff and ensure consistency. The chief information officer should also update the department's strategic plan.

The department should update its offsite storage policy. COBIT identifies offsite storage of critical backup media, documentation, and other technology resources as a control to ensure continuous service. Department policy requires backup media to be sent offsite no later than 48 hours after the data backup is completed. However, DIT staff told us the city's current contract with the offsite storage vendor provides for pickup once every two weeks. The chief information officer should update the department's backup policy to reflect its current contract.

The department should document job scheduling controls. COBIT identifies efficiently sequencing scheduled jobs, processes, and tasks as a control to meet business requirements. The department has scheduled 15 data transfer jobs in Oracle, including financial, medical coverage and employee benefit information. While the department limits access to job scheduling to a few individuals, it has no policy for changing scheduled jobs. The chief information officer should document procedures regarding sequencing and scheduling jobs.

The department should update its strategic plan. COBIT identifies a strategic plan as a necessary control to manage information technology resources in line with the entity's overall business strategy and priorities. The strategic plan should assess current performance and identify capacity and human resource requirements. The department's most recent strategic plan covers the period 2004 through 2006. While some of the plan elements remain current, others are out-of-date. For example, the plan identifies selecting an ERP system as a strategic objective. The city implemented Oracle in 2008. Focus has since shifted from procurement and implementation to ongoing maintenance. The chief information officer should update the plan to reflect the city's current needs.

Staff Did Not Follow Some Policies that Would Reduce Risk

While the department has established procedures to manage user accounts and change management policies to protect city data, failure to follow or enforce policies poses risk. Staff failed to remove hundreds of employees' access to city systems when they left city employment, increasing risk of unauthorized access to sensitive data, misuse of data, or fraud. Staff also failed to document approval of a technical change to Oracle. Changes to technology systems are inherently risky; reviewing and approving changes in a consistent and coordinated way reduces the likelihood that changes will disrupt a system.

Hundreds of former city employees had access to systems months after leaving city employment. Failure to close unused accounts weakens system security and increases risk of unauthorized access to sensitive data, misuse of data, or fraud. External sources could exploit the weakness to gain access to the system or current users could evade accountability by accessing the system using a former employee's ID. We reviewed system access for the 496 employees who left city employment between December 2008 and December 2009:

- 287 still had access to Oracle
- 105 still had network access
- 2 still had access to Kronos
- 3 still had access to Oracle's operating system
- 1 still had physical access to restricted areas of the building

Six of the Oracle userids and 27 of the network userids were accessed after the termination dates.

Under the city's employee separation process, the Department of Information Technology removes system access for a former employee once the department receives an employee separation or suspension notification from Human Resources or from an employee's supervisor. Department staff told us they are not always notified of separations. We recommend the chief information officer work with the director of human resources to ensure the department is promptly notified when employees leave city employment. The department should also periodically review and validate the list of employees with access to each city system.

The Department of Information Technology removed system access for the Oracle operating system accounts and the past employee with access to restricted areas of City Hall we identified. However, city systems remain at risk for unauthorized access. We tested specific systems over a defined period. Given the number of problems we found and similar findings in our previous work on watershed and aviation applications, it is likely that separation procedures have not been followed since we completed our tests.

Technical change document was incomplete. We reviewed a judgmentally selected technical change document for a request to apply a patch to the Oracle financial module to correct a problem with accumulated encumbrances. The document lacked a contingency plan if the change was unsuccessful and lacked evidence of committee approval. According to city policy, each scheduled change request must be approved before implemented and the change control board may deny requests that have inadequate back out plans.

Changing a system is inherently risky. Change management should ensure that all changes are logged, assessed and authorized before implementation and reviewed against planned outcomes after implementation in order to mitigate risks of destabilizing the system or other unintended consequences. We recommend the department verify all system changes and document approval prior to implementation.

No Policy or Practice for Over One-Fourth of Needed Controls

The Department of Information Technology has no policies or practices to cover 28% of the control objectives that we reviewed from the COBIT framework. The department lacks disaster recovery and business continuity plans, procedures to monitor security logs, procedures to test backups, assessment of legal and regulatory requirements, and service agreements with other departments. The department does not enforce the city's guidelines for strong passwords in the Oracle system. These weaknesses increase security, compliance, and performance risks. We recommend the department develop a disaster recovery plan. We also recommend the department work with the law department to identify regulations applicable to city data and systems and establish service level agreements with city departments. We provided the chief information officer specific recommendations to enhance system security in April 2010.

The city is vulnerable to a prolonged service interruption. Although the city has a disaster recovery plan for its mainframe computer, which houses some systems used by police and the court, it lacks plans for critical systems that reside on servers, including Oracle, Kronos, the 911 dispatch system, the city's radio system, and email. COBIT identifies business continuity and recovery plans as key aspects of controls to ensure continuous service. Planning for disasters and testing to be sure the plan works can reduce costs and the time needed to restore service. Plans usually specify where equipment would be relocated, the source of emergency equipment and backup data, contact lists with areas of responsibility, and the priority in which to restore critical systems. The chief information officer should evaluate options and seek funding to develop business continuity and disaster recovery plans for the city.

Backup procedures should include periodic testing. The department lacks procedures to periodically test backups and was unable to restore previously deleted emails for a user during our audit tests. COBIT identifies periodic tests to ensure that all components of backups can be effectively restored as a component of effective backup and restoration controls. The department should regularly test its ability to restore data.

Strong password policy not enforced in Oracle. The department does not enforce the city's guidelines for strong passwords in Oracle. Unlike network passwords, Oracle passwords can be less than eight characters and never expire. In addition, the department issues the same generic password to all new users. Passwords are a means of authenticating users so that only authorized users can access system data, and system records of who performed various functions are accurate. Weak passwords provide less protection from unauthorized access or changes to key financial data and programs. COBIT identifies enforcing password rules as a key component of ensuring system security. While strong network passwords help to protect Oracle from external sources, because users must log on to the network before logging on to Oracle, weak passwords make Oracle more vulnerable to internal threats. The chief information officer should strengthen password requirements applicable to Oracle.

Security logs not monitored. The department lacks procedures to review the AIX-Oracle operating system security logs. COBIT identifies actively testing and monitoring IT security implementation as a control objective for ensuring system security. Logging and monitoring enables early detection and subsequent timely reporting of unusual activities that may need to be addressed. The chief information officer should implement a procedure to periodically review security logs.

The city faces compliance risks. The city has yet to identify legal regulations and standards applicable to city data. Sensitive data, such as employee and customer information, may be protected by regulations and its mishandling presents a liability risk. Continuously identifying laws, regulations, and other external compliance requirements for incorporation into the organization's policies, standards, procedures and methodologies is a key control objective in COBIT for monitoring and evaluating system design and controls.

State and federal laws and regulations may apply to city operations. For example:

- O.C.G.A § 10-1-393.8 addresses rights of protection from disclosing an individual's social security number.
- GPIPA (Georgia Personal Identity Protection Act) requires notification to individuals whose personal information has been breached. Government agencies with records related to traffic safety, law enforcement, and licensing are exempt.
- Red Flags Rule (Federal Trade Commission) applies to identity theft from utilities among other groups. The city would have to institute a red flag program to prevent and detect identity theft.

The chief information officer should work with the city attorney to identify laws and regulations that apply to city data. The chief information officer should develop procedures to classify and protect data commensurate with requirements.

Service guidelines are not defined. The Department of Information Technology has not established service level agreements with each department it serves to define expected services and promote accountability. COBIT identifies service level agreements as a key control for defining and managing services to meet business needs. Service level agreements usually cover customer commitments; service support requirements; quantitative and qualitative measures of services; roles and responsibilities, including oversight of the agreement; and sometimes cover funding mechanisms. Items to consider in developing agreements include availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints. The chief information officer should enter into formal service level agreements with each department served to promote service accountability.

Department Appears Understaffed but Staffing Plan Overstates Need

The department estimated it needed an additional 85 staff — more than double its current level — in a December 2009 presentation prepared for the new administration and City Council. While we agree that the department appears to be understaffed, omissions and errors in the analysis overstated staffing needs in some areas and understated staffing needs in others. Although the presentation purported to use industry standards to identify staffing needs, more than half of calculations were based on staff's professional judgment and some data used in calculations lack support. We estimate that the department needs an additional 49 staff members based on industry standards and data that we could verify.

The chief information officer should assess staffing levels in conjunction with updating the department's strategic plan and developing service level agreements with operating departments. Staffing should be consistent with resource requirements identified in these documents.

The Plan Overstates Needs in Some Areas and Understates Need in Others

Reapplying the department’s method with corrected data and benchmarks, we estimate the department needs 49 additional staff. The department overstated staffing need primarily by excluding contractors from its count of current staff. The department undercounted staffing needs in some areas compared to staffing ratios compiled in the 2009 *IT Staffing Ratios* report by Computer Economics, which the department cited as its source for industry standards. In some cases, the department reduced the calculated number of staff required due to concern that the calculated figure was too high to be politically feasible.

The presentation overstated staffing need by excluding the department’s 30 contractors from the calculations. The department reported in a December 2009 presentation prepared for the new administration and City Council that it needed 85 additional staff to be consistent with industry standards (see Exhibit 4). However, the analysis excluded contractors. As of November 2009, when the analysis was completed, the department had 81 budgeted positions and employed another 30 consultants. Seven of the budgeted positions were vacant. Consultants supported 10 of the 14 “departments” referred to in the presentation, but were not counted within the number of employees.

Seven of 14 calculations were based on industry standards. Although the presentation purported to reflect “accepted industry metrics,” only seven of the 14 calculations included in the presentation used the key measures from the 2009 *IT Staffing Ratios* report, which the chief information officer identified as the basis for the department’s analysis. The department calculated staffing need in four areas based on a different measure than the ratio used in the report:

- Project Management
- Network Support
- DBA Support
- ERP

Applying different ratios to estimate need resulted in higher staffing calculations in Project Management and DBA Support and resulted in lower staffing calculations in Network Support and ERP. Staff told us the department reduced the number of staff needed in these latter areas due to concern that the calculated figure was too high to be feasible. Also, staff was trying to estimate only the number of additional trainers and help desk staff needed to support ERP rather than all ERP support staff.

The 2009 *IT Staffing Ratios* report provided no staffing measures for Telecommunications, Inventory Management, and Data Center Operations. Staff told us that the department applied ratios from the report that seemed applicable to Telecommunications and Inventory Management and that professional judgment was the basis for the Data Center Operations estimate.

Some staffing calculations were based on outdated, inconsistent or unsupported data. The department estimated the number of server support staff needed based on the number of city servers in use. However, the department consolidated applications and reduced the number of city servers requiring support from 420 to 335 during the time of the study. The department estimated the number of help desk, application support, internal security, and ERP staff needed based on the number of city users, but which ranged from about 4,687 to 8,000. Staff in different functional areas told us that they estimated the number of users in different ways and were not able to provide support for their estimates. The department estimated the number of telecommunications support staff needed based on numbers of mobile devices, telephone sets, and telephone systems in use in the city, but were unable to provide support for their estimates. We also identified a few calculation errors in the department's presentation.

Exhibit 4 shows our recalculation of the department's staffing gap after adding the contractors, applying industry standards that we could verify, and applying a consistent count of city users. We estimate a staffing gap of at least 49 staff and identified four areas, marked in blue, where the department's presentation understated need and five areas, marked in pink, where the department's presentation overstated need.

Exhibit 4 Recalculation of Staffing Need

Functional Unit	Key Benchmark	Current Staff	Contractors	Staffing Gap Calculated by Auditors	Staffing Gap Reported by DIT
Project Management	Project managers as a % of IT staff	7	1	-5	12
Telecommunications	No key benchmark	4	2	N/A	11
Server Support	Servers per server engineer	7	2	7	3
Network Support	Desktops per network engineer	2	1	9	2.5
Inventory Management	No key benchmark	1	0	N/A	1
Data Center Operations	No key benchmark	4	3	N/A	7
Desktop Support	Desktops per engineer	10	4	0	3.5
Helpdesk	# of users per help desk employee	6	0	12	9
Application Support	# of users per application employee	19	2	15	18
DBA Support	% of IT staff	2	2	1	2
ERP	# of users	2	12	N/A	6
Security	# of users	1	0	4	4
Business Office Support	Finance/clerical staff as a % of IT staff	4	1	-1	2
Management	# of employees managed	9	0	7	4
	TOTAL	**78**	**30**	**49**	**85**

Source: Analysis of the plan, verification of key benchmarks, and review of the Computer Economics survey

🟥 Overstated need   🟦 Understated need   🟨 Could not calculate

We did not estimate the number of ERP staff needed because ERP support duties are marbled throughout the department rather than confined to a single business unit. To estimate the number of city users the Department of Information Technology supports, we counted the number employees as of March 2010 and excluded Department of Aviation and Department of Watershed Management employees because these departments operate internal information technology units. We also excluded employees who perform jobs that do not require work on a computer such as landscaping, street cleaning, tree trimming, yard waste removal and rubbish collection.

The chief information officer should re-assess staffing levels while updating the department's strategic plan and developing service level agreements with operating departments. Staffing should be consistent with resource requirements identified in these documents.

The Department Has Made Progress Implementing Recommendations

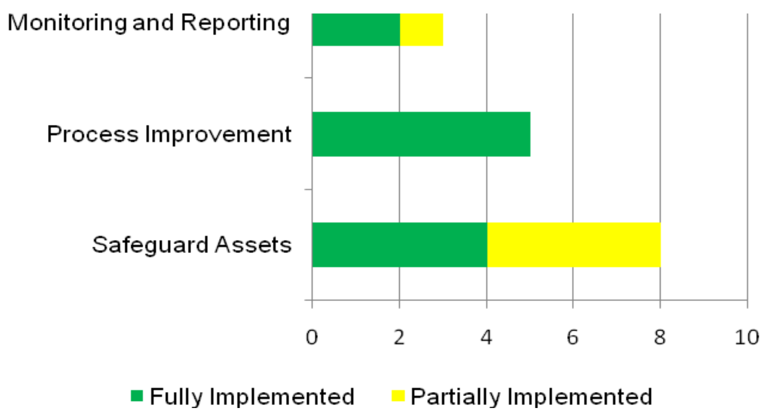
The Department of Information Technology has implemented 11 of the 16 recommendations that we assessed, and is working to complete implementation of the remaining five recommendations. The department has strengthened change management, data reliability and integrity, and knowledge transfer from contractors.

While the department developed a report to identify potential payroll errors, as we recommended in our 2008 performance audit, *Review of the Oracle ERP First Payroll Run,* the report we reviewed for the pay period ending April 14, 2010, was incomplete, resulting in undetected errors. The city underpaid five employees a total of $1,145. The city overpaid one employee $276; the report correctly flagged the error but staff did not correct the error before processing payroll. We recommend the chief information officer work with payroll to develop a process to reconcile all differences between Kronos and Oracle before processing payroll.

The Department Has Implemented Most Recommendations

The department has fully implemented 11 of the 16 recommendations we assessed. The department has partially implemented the remaining five recommendations and is working to complete the implementation. Most recommendations dealt with safeguarding assets and improving processes (see Exhibit 5).

Exhibit 5 Implementation Status by Risk Area



Source: Assessment of Implementation of Audit Recommendations

Eight of 12 Oracle recommendations implemented. In the June 2007 performance audit, *ERP Implementation Assessment,* KPMG recommended documenting changes to the system, capturing knowledge from contractors, developing a strategy for patch management, and providing job aides for users. The department tracks changes to Oracle through its helpdesk system and documents the changes. The department pairs its staff with the consultants and records problems and resolutions to ensure that city staff can support Oracle once the consultants leave. The change management policy and change control board help manage patches and upgrades. The department provides a website for users to practice with Oracle and learn basic navigation.

One of two 911 system recommendation implemented. In our 2008 performance audit, *Police Computer Aided Dispatch Data Reliability*, we recommended that the chief information officer direct Northrop Grumman to correct programming errors for response time and dispatch delay reports. Northrop Grumman maintains the dispatch system for the police department. About 2% of 911 calls were excluded from the reports because the calls spanned midnight. Northrop Grumman created a process to validate the change in date so the calls would be included. We tested one call and found it in the reports.

Two of two Oracle payroll recommendations implemented. In the 2008 *Review of the Oracle ERP First Payroll Run* audit, we recommended that the chief information officer develop controls to detect errors in Kronos. We also recommended that the chief information officer analyze errors in Kronos and work with the Controller to address areas of recurring misuse. Incorrect use of the city's timekeeping system, Kronos, resulted in overpayments of about $243,000 in overtime. The department created a report to help payroll identify discrepancies between Kronos and Oracle and hired a Kronos consultant to suggest ways to reduce discrepancies. We analyzed the first payroll for April 2010. While the report identified 64 errors — of which payroll corrected 63 — we found additional errors not included in the report.

The department plans to implement the remaining recommendations. In the *ERP Implementation Assessment*, KPMG recommended that the department keep Oracle source files in a secure common repository, track system changes, and analyze system needs before purchasing additional servers. KPMG noted risks that Oracle could not be fully restored without the files and changes, and that servers may not work well enough or need to be replaced sooner than expected.

The department is working to address the remaining recommendations. The department is looking for software to maintain Oracle file versions and automatically track system changes and plans to evaluate which servers it needs to replace.

In the *Police Computer Aided Dispatch Data Reliability* report, we found multiple gaps in incident numbers within the system. We recommended that the chief information officer direct Northrop Grumman to investigate the gaps and whether records were missing. Northrop Grumman responded that the system had been used to train staff and those entries were then deleted. The city's 911 system may become unstable if test records are not separate from the live calls. Northrop Grumman plans to create a version of the system for training staff by September.

Timekeeping Continues to Pose Risk

While the department developed a report to identify potential payroll errors, as we recommended, the report we reviewed was incomplete and failed to identify overtime underpayments. The chief information officer and the controller should establish a process to reconcile all differences between Oracle and Kronos each pay period before processing payroll.

The department and payroll should reconcile overtime. In the *Review of the Oracle ERP First Payroll Run* audit, we recommended that the chief information officer implement controls to confirm data in Kronos and work with payroll to address recurring errors. Timekeepers had been entering overtime into Kronos incorrectly, creating overpayments in Oracle. The department created a report that identifies where overtime hours in Oracle are greater than the corresponding time entries in Kronos. Each cycle, payroll staff manually corrects the entries in Oracle based on the report.

Although the process the department developed identifies instances where overtime hours in Oracle lack matching entries in Kronos, we found additional overtime errors in the payroll we tested for the pay period ending April 14, 2010. The city underpaid five employees a total of $1,145 which payroll believes occurred because timekeepers entered the overtime incorrectly in Kronos. The city overpaid one employee $276; the report correctly flagged the error but staff did not correct the error before processing payroll. The report also listed 404 valid overtime entries —overtime hours in Oracle matched the overtime hours in Kronos. The report excluded 2,601 overtime entries, which also appeared to be valid. It's not clear why the report listed some but not all valid overtime entries.

We recommend that the chief information officer work with the controller to develop a process to reconcile all differences between Kronos and Oracle before processing payroll. The process should be automated to the extent possible, but if payroll staff must make manual corrections, the payroll director should review corrections for accuracy.

Recommendations

The chief information officer should:

1. Update department policies to strengthen security and to reflect actual practices in order to clarify expectations of staff and ensure consistency. The update should include:
   - documenting procedures regarding sequencing and scheduling jobs
   - ensuring the backup policy reflects its current contract
   - regularly test its ability to restore data
   - periodically reviewing security logs
   - periodically reviewing and validating the list of employees with access to each city system
   - strengthening password policies applicable to Oracle

2. Update the department's strategic plan to reflect the city's current needs. The plan should include staffing needs, contractor support, and clearly indicate the basis for its calculations.

3. Work with departments to establish service level agreements consistent with the department's updated strategic plan.

4. Evaluate options and seek funding to develop business continuity and disaster recovery plans for the city.

5. Ensure that approval for system changes is documented prior to implementation.

6. Work with the city attorney to identify laws and regulations that apply to city data and develop procedures to classify and protect data commensurate with requirements.

7. Work with the controller to establish a process to reconcile differences between Kronos and Oracle.

8. Work with the commissioner of human resources to ensure the department is notified when employees leave city employment to enable prompt removal of user access to city systems.

Appendices

Appendix A
Management Review and Response to Audit Recommendations

Report # 09.07	Report Title: Information Technology General Controls	Date: 10/21/2010

Recommendation Responses

Rec. #1		
	The chief information officer should update department policies to strengthen security and to reflect actual practices in order to clarify expectations of staff and ensure consistency. The update should include: • documenting procedures regarding sequencing and scheduling jobs • ensuring the backup policy reflects its current contract • regularly test its ability to restore data • periodically reviewing security logs • periodically reviewing and validating the list of employees with access to each city system • strengthening password policies applicable to Oracle	Agree

Proposed Action:

1. Documenting procedures regarding sequencing and scheduling jobs:

All ERP modules related jobs are created and run by functional staff, who have the appropriate security rights to do so. The DBA team will monitor processes to make certain such jobs do not impact the environment. However, the decision to create and run these jobs is driven by the business owners.

2. Ensuring the backup policy reflects its current contract:

The City's backup policy requiring backup tapes to be shipped out within 48 hours has been changed to two (2) weeks to align with the City's current contract with the tape storage vendor, Recall.

3. Regularly test its ability to restore data:

We have revised the backup and restore procedures and document tests of our restoration process.

4. Periodically reviewing security logs:

We have created procedures for reviewing the Oracle operating system and other similar operating system security logs.

Proposed Action:

5. Periodically reviewing and validating the list of employees with access to each city system:

DIT has cleaned up/removed the 200 employees who at one point in time retained access to Oracle and the network. In addition, DIT has been working with the human resources personnel to ensure the department is made aware when employees leave city employment to enable removal of user access to city systems and to strengthen policies relative to this matter.

6. Strengthening password policies applicable to Oracle:

Along with the ERP Functional Leads and S&P staff, the following decision has been made:

- Require Oracle password reset on a 45 day schedule
- Profile options that will be implemented include:
  - ➢ Signon password failure limit
  - ➢ Signon password hard to guess (containing at least one letter; at least one number; does not contain the user name; and does not contain repeating characters)
  - ➢ Signon password length
  - ➢ Signon password no reuse
  - ➢ Signon password case

- We will choose the mid-November as an implementation date; we are sensitive to having recently required CoA employees to access their payslip information on line and want to give a few more paycycles to cement.

  Note: though there is a password reset functionality in Oracle, we may require assistance for the Help Desk to handle potential increased demand; we will begin development testing of this functionality.

- We are working on the communiqué for City employees that should go out within the next two (2) weeks

Implementation Timeframe:

Completed#: 1, 2, 3, 4; 5 DIT will be working with the Human Resources Department to address this issue; 6 will be completed mid- November.

Responsible Person:

Kim Bolarinwa, Ken Amakor, Jeremy Johnson, Jaci Vickers, respectively

Rec. #2	The chief information officer should update the department's strategic plan to reflect the city's current needs. The plan should include staffing needs, contractor support, and clearly indicate the basis for its calculations.	Agree
Proposed Action:	The CIO has developed a three-year Strategic Plan to reflect the City's current business needs. The Strategic Plan reflects the Mayor's Strategic Focus Areas and overall budgetary needs to execute specific projects to achieve his Strategic Focus Areas over the next three years.	
Implementation Timeframe:	Complete	
Responsible Person:	Dan Smith	
Rec. #3	The chief information officer should work with departments to establish service level agreements consistent with the department's updated strategic plan.	Agree
Proposed Action:	The Strategic Plan addresses the IT Consolidation Initiative that consolidates the Department of Information Technology, Department of Watershed Management IT and Department of Aviation IT. Key deliverable from the IT Consolidation Initiative is the establishment of service level agreements consistent with the department's updated strategic plan.	
Implementation Timeframe:	TBD based upon the IT Consolidation Initiative	
Responsible Person:	Dan Smith	
Rec. #4	The chief information officer should evaluate options and seek funding to develop business continuity and disaster recovery plans for the city.	Agree
Proposed Action:	The CIO is currently working to develop a disaster recovery RFP which initial funding has been allocated to this initiative. Additional funding is required; the implementation of DR & Business Continuity Plans will expand over a three years period. City of Atlanta will need to identify a Business Continuity Champion. The DR plan is not effective without the Business Continuity Plan.	
Implementation Timeframe:	TBD	
Responsible Person:	Dan Smith	

Rec. #5 The chief information officer should ensure that approval for system changes is documented prior to implementation.

Agree

Proposed Action: Change management control is essential to safeguarding the integrity of the production environment. Policies and procedures to guide appropriate DIT staff in this regard have been developed, disseminated and discussed.

To ensure system changes are documented and validated for approval prior to migration into production, DIT relies on the following activities:

- Weekly Change Management meetings that involve a review of each request (patch, etc.) is conducted; the assessment must include review of all test results from both a development and the quality assurance instance.

- Requirement and documentation that essential support staff (e.g., ERP Program Director) are participants in these weekly Change Management calls; approval must be also provided by these staff.

- Follow-up approval confirmation is sent to the Database Administrators (DBAs) and others by the Change Board Administrator or designee; the DBAs, in turn, review all documentation before migration into production.

To augment the procedures listed above, DIT is currently assessing the use of software which will be used to track, among other things, database and application changes and licenses. Furthermore, DIT is currently assessing automated testing to improve the timeliness of these efforts.

Implementation Timeframe: Complete

Responsible Person: Ken Amakor

Rec. #6 The chief information officer should work with the city attorney to identify laws and regulations that apply to city data and develop procedures to classify and protect data commensurate with requirements.

Agree

Proposed Action: DIT has reached out to the Law Department to identify laws and regulations that apply to city data. The Law Department is researching the laws and regulation for compliance. DIT will work with the Law Department to develop procedures to classify and protect data.

Implementation Timeframe: TBD

Responsible Person: Ken Amakor

Rec. #7	The chief information officer should work with the controller to establish a process to reconcile differences between Kronos and Oracle.	Agree
Proposed Action:	The CIO will work with the Controller to establish a process to reconcile differences between Kronos and Oracle.	
Implementation Timeframe:	Dependent upon Controller's availability & priority	
Responsible Person:	Kim Bolarinwa, Jaci Vickers & Controller	
Rec. #8	The chief information officer should work with the commissioner of human resources to ensure the department is notified when employees leave city employment to enable prompt removal of user access to city systems.	Agree
Proposed Action:	DIT has been working with the human resources personnel to ensure the department is made aware when employees leave city employment to enable removal of user access to city systems and to strengthen policies relative to this matter. We will continue work with Human Resources Commissioner and personnel.	
Implementation Timeframe:	Dependent upon Human Resources Commissioner's availability & priority	
Responsible Person:	Kim Bolarinwa, Ken Amakor & Jeremy Johnson	

Appendix B
Implementation of Audit Recommendations by Risk Category

Risk Area	Report Title and Date	Recommendation	Implementation Status
Monitoring and Reporting	Review of the Oracle ERP First Payroll Run April 2008	The Chief Information Officer should implement detect/validation controls. Focus for these controls needs to be on the Kronos system as this is where the errors are occurring. These controls should be automated/semi-automated. Checks should analyze all errors (OT, UXT transfers, Regular time over 80 hours etc.).	Fully Implemented
Monitoring and Reporting	Police Computer Aided Dispatch Data Reliability April 2008	The chief information officer should direct Northrop Grumman to correct report programming errors and ensure that report programming accurately captures all relevant records.	Fully Implemented
Monitoring and Reporting	Police Computer Aided Dispatch Data Reliability April 2008	The chief information officer should direct Northrop Grumman to investigate why there are gaps in incident numbers, determine whether records are missing, and if so, whether system or operating changes are necessary to resolve the problem.	Partially Implemented
Process Improvement	ERP Implementation Assessment June 2007	Capitalize on the knowledge of the external consultants to leverage additional expertise until in-house subject matter experts are developed.	Fully Implemented
Process Improvement	ERP Implementation Assessment June 2007	Add one experienced Oracle SR DBA to the two DBAs listed. Immediately begin to cross train DBAs from other applications for emergencies. Leverage the external contractors to bolster complicated tasks and transfer knowledge in-house.	Fully Implemented

Risk Area	Report Title and Date	Recommendation	Implementation Status
Process Improvement	ERP Implementation Assessment June 2007	Team internal COA employees with external contractor to ensure there is adequate knowledge transfer. Ensure that all contractor services are documented and turned over to the COA as a deliverable. Ensure adequate oversight of contractor activities. Maintain complete, accurate and current documentation in a secure repository.	Fully Implemented
Process Improvement	ERP Implementation Assessment June 2007	Distribute a reporting catalogue to the end user population on a recurring basis. Initially, this can be laminated and provided to each user as a reference guide. The reporting catalogue should be updated as information is changed or reports are added. As new reports are added, an updated reporting catalogue can be re-distributed. In addition, end users should also have the ability to access the reporting catalogue electronically. The reporting catalogue should contain the following information: report name, report description, business purpose, report folder location, information related to the rows and columns, when the report is available on a recurring basis, report owner.	Fully Implemented
Process Improvement	ERP Implementation Assessment June 2007	Job aids, checklists and end user flow charts should be developed to support the end users in their daily, monthly and quarterly responsibilities. Job aides can serve as a quick reference or "how to" guide. Checklists can help the end user understand all the activities that need to be performed on a recurring basis. End user flow charts are very useful for users to gain a better understanding of the end to end process and possible downstream implications of incorrect transactions.	Fully Implemented

Risk Area	Report Title and Date	Recommendation	Implementation Status
Safeguard Assets	ERP Implementation Assessment June 2007	Each time a modification/configuration is made to the production environment, a corresponding instruction document should be created. Ideally, it should have screen prints of changes and steps to recreate the change. For example, a SQL based Oracle Alert should also clearly document the SQL code used. File directories and database settings are unique to each system. Instructions that delineate the steps, directories and any functional updates such as profile option settings are crucial to restoring the instance and should be documented. The documents should be securely stored on a common repository and its location added to the updated customization list. Additionally, include the completion of modification documents as a check-off item in the Change Management process.	Fully Implemented
Safeguard Assets	ERP Implementation Assessment June 2007	Assign at least one employee and one backup employee the responsibility of maintaining the list of modifications and customizations that are applied to the production environment. The list should include: latest date of change, where the source code is stored, module updated, change in functionality, who approved the change, location of implementation instructions, whether it is registered in Oracle. The list should be reviewed for accuracy at least once a year and during upgrades by the Department of Information technology and functional users. The list should be stored on a secure repository such as iProjects.	Fully Implemented

Risk Area	Report Title and Date	Recommendation	Implementation Status
Safeguard Assets	ERP Implementation Assessment June 2007	A strategy must be developed and followed to address applying patches and upgrades for the end users. Patches and upgrades must be approved by a Change Control Board (CCB) and tested in a test environment prior to movement into a Production environment. Post implementation acceptance testing must be conducted after the patch or upgrade is applied to the production environment. Post implementation acceptance testing must be conducted after the patch or upgrade is applied to the production environment. Key business users need to be trained on the use of Metalink (Oracle's support portal). Oracle does not deploy patch information to the client base. Customers of Oracle applications must frequently poll Metalink for the information or register for the monthly newsletters or alerts. It is recommended that at least two key business users from each department enroll for these newsletters.	Fully Implemented
Safeguard Assets	Review of the Oracle ERP First Payroll Run April 2008	The chief information officer should facilitate the analysis of errors that occur or continue to occur in the Kronos system and work with the Controller to devise courses of action to address recurring misuse	Fully Implemented
Safeguard Assets	ERP Implementation Assessment June 2007	Any future hardware purchases should be made after a thorough analysis and testing outlined in other recommendations in this report.	Partially Implemented

Risk Area	Report Title and Date	Recommendation	Implementation Status
Safeguard Assets	ERP Implementation Assessment June 2007	A clear list of all modifications that would be over written should be maintained as a part of the patch management system. Additionally, form changes and customized concurrent programs can be registered in Oracle so they will not be over written during upgrades and patching.	Partially Implemented
Safeguard Assets	ERP Implementation Assessment June 2007	Source files should be stored in a secure common repository along with the instructions outlined in Observation 2.1.5.2, if applicable. File versioning should be maintained and new file versions should be saved along with the older versions and not overwritten. Additionally, access should be limited to those who would use the files.	Partially Implemented
Safeguard Assets	ERP Implementation Assessment June 2007	To validate the adequacy of the purchased hardware it is imperative that the COA develop a robust and detailed performance test plan. The performance testing should include the following criteria: performed on the actual production servers with all production data and settings; use anticipated peak transaction volumes as throughputs to measure CPU, memory usage, and response times; a timeline of when reports, concurrent programs and interfaces will be processed should be created; varying peak times for processes such as open enrollment, supplier reporting, expense submission, and so on should be built into the plan to help anticipate non-daily performance impacts; transition impacts from inside and outside the COA network should be tested due to the significant emphasis on self-service products such as iExpense, iSupplier, and iReceivables.	Partially Implemented