DEKALB•COUNTY•GEORGIA

1822

Internal Audit Division
Finance Department
DeKalb County

REVIEW OF GENERAL INFORMATION TECHNOLOGY SYSTEM CONTROLS

DECEMBER 2016

Page intentionally left blank

Finance Department
Internal Audit Division

TRANSMITTAL MEMORANDUM

DATE: December 22, 2016

TO: John Matelski, Director of Innovation and Technology

FROM: Cornelia Louis, Deputy Director Finance – Internal Audit Division

SUBJECT: Department of Innovation and Technology

RE: Review of General IT System Controls

Attached is the report of the General Information Technology (IT) System Controls review. General IT controls are controls in the environment surrounding information systems. These controls can include separation of duties, adequate safeguard of the County's information systems, program and data security, and computerized backup and recovery of computer operations. Our review of general controls found opportunities for improvements, which were discussed with you during the Exit Conference on December 22, 2016.

Management's responses to our audit observations and recommendations are included in the following report.

If you have any questions about the audit or this report, please feel free to contact me at 404-371-2639.

Sincerely,

Cornelia Louis

Cornelia Louis

cc: Appendix D

Table of Contents

EXECUTIVE SUMMARY

General Information

"General controls apply to all systems components, processes, and data for a given organization or system environment. General controls include, but are not limited to, IT governance, risk management, resource management, IT operations, application development and maintenance, user management, logical security, physical security, change management, backup and recovery, and business continuity."[1]

The Department of Innovation and Technology (DoIT) consists of a Chief Innovation and Information Officer who oversees four divisions: Business Solutions, Infrastructure and Operations, IT Security Operations, and Strategic Support. DoIT' s adopted budget for 2016 was $22,510,677 with 79 full-time (FTE) staff. As of November 2016, 69 full-time positions have been filled. Please see **Appendix C** for a description of each division.

Most departments rely on DoIT for application and customer support. However, some DeKalb County departments including elected official offices have one or more assigned system administrators who may typically perform Information Technology (IT) functions (e.g. modify accounts in the Active Directory). These department administrators can only view data for their respective departments. In addition, Superior Court Administration provides technology support for all Superior Court programs and courtrooms, including computer systems for staff.

The County's Active Directory includes three network domains in which the following resides:
Superior Court – user accounts and servers
Computer Aided Dispatch (CAD)/E-911 – CAD software
DeKalb County Government (DCG) – majority of all user accounts including Police and 911 employees, and excluding Superior Court

The DoIT is responsible for supporting information technology of the County day-to-day operations and is the County's central IT. Therefore, there is a two-way trust between the responsible parties for changes and modifications made in each domain. In addition, there is a standing order from DeKalb County Superior Court that their consent is required for changes to any existing policy or access control lists that is either inherited or directly applied to Superior Court Storage Group in the DeKalb County Exchange email system or Superior Court domain.

Objective, Scope, and Approach

The overall objective of the audit is to assess information technology general controls within DoIT. The audit did not include a review of the telecommunications controls. Moreover, the business continuity component of IT general controls was addressed in Internal Audit's Emergency Management Review.

[1] GTAG-1: Information Technology Risk and Controls 2nd Edition, Institute of Internal Auditors, Altamont Springs, Fla., USA 2012

The period covered is January 1, 2015 through December 31, 2015. The scope of the audit is to determine the following:

1. Access to programs and data is properly restricted to authorized individuals only.
2. All changes to existing systems are properly authorized, tested, approved, implemented, and documented.
3. New system/applications being developed or implemented are properly authorized, tested, approved, implemented, and documented.
4. IT supported system and programs/applications are available and processing accurately.

To meet the audit objectives, Internal Audit requested that DoIT complete an internal control self-assessment, interviewed management and staff, conducted site visits, observed and assessed processes, reviewed policies and procedures, and reviewed available documentation.

Summary of Observations

1. The Disaster Recovery Plan (DRP) is outdated and no recent recovery test has been performed
2. Infrequent monitoring to ensure backup completes
3. Backup tapes not properly secured and infrequently delivered to storage site
4. IT Security lacks direct access to the software system used to help safeguard assets
5. Limited monitoring of access controls over user accounts
6. No configuration of password control in Oracle
7. Help Desk system enhancement needed
8. Control weaknesses identified in Change Management process
9. Control weaknesses identified in Application Implementation and Upgrade process

Overall Recommendation and Next Steps

Strengthening controls over the County's information technology ensures data is protected and available to meet daily business needs.

Summary Management Response

Overall, management concurs with the audit recommendations and has implemented corrective action or plans to implement corrective action regarding IT general controls over the County's information systems and data.

Approvals:

Original Signed by:

Cornelia Louis

Cornelia Louis
Deputy Director of Finance
Internal Audit Division
Department of Finance
DeKalb County

SUMMARY OF OBSERVATIONS

1. The Disaster Recovery Plan is Outdated and No Recent Recovery Test Have Been Performed

DoIT disclosed tests to determine if systems and data are available in the event of a disaster have not been performed since 2014. However, we did not receive copies of the test results or a copy of the Disaster Recovery Plan (DRP); therefore, we could not comment on its existence, accuracy, or effectiveness. Moreover, a recent internal review of DoIT Continuity of Operations Planning (COOP) identified opportunities for improvement.

Recovery testing is part of business continuity planning. Recovery testing of backup data is critical to ensuring availability of the data and minimal disruption to business operations, in the event of a disaster. Per the Institute of Internal Auditors (IIA), *Global Technology Audit Guide*: *Business Continuity Management,* "the generally accepted leading practice is for the frequency of the business continuity management to be sufficient to ensure that the program is becoming progressively more mature."[2] The DoIT File Server policy includes expectations for backup and data restoration; however, the language is specific to restoration for individual situations where a department may need data restored.

Recommendation

DoIT should perform system recovery tests and update policies to include periodic performance of every test to ensure continuation of operations in the event of a disaster. Additionally, documentation should be maintained to support performance of the tests and for monitoring the process.

Management Response

DoIT concurs with this recommendation. DoIT is in the process of updating associated policies as a function of the County's Continuity of Operations Planning (COOP) process that is spearheaded by the DeKalb County of Emergency Management Agency (DEMA). We will have up to date policies and documentation by the end of this year (2017). It is also the intent of DoIT to establish disaster recovery testing for mission critical systems, as a function of the 2018 budgeting process. The ability to resume disaster recovery testing is a function of funding availability, and other technology innovation and modernization efforts that support the county's strategic initiatives have taken priority.

2. Infrequent Monitoring to Ensure Backup Completes

Cloud computing is used by DoIT for some of its storage solutions. It is a convenient way for service providers to offer applications and services over the Internet with minimal effort from management and service provider interaction. We observed an instance where a few servers showed some missing data in a report that documents the last backup date. For one server there was no data documented in the field denoting the last backup date, which DoIT staff indicated was concerning. When asked about the frequency of monitoring, DoIT staff disclosed monitoring is not performed as preferred due to other priorities and the time

[2] Business Continuity Management, Institute of Internal Auditors, Altamont Springs, FLA., USA 2008

it takes to research potential issues. The DoIT File Server Policy provides guidelines for backing up data and expectations are that backups will be complete as the policy states, "The file servers are backed up on a daily basis and full backups are done monthly."

County departments rely on DoIT to ensure information systems are operating and data will be available to meet their business needs. Lack of frequent monitoring to ensure completion of the backup processes, along with untimely resolution of potential issues could lead to other problems within the system. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework on Monitoring Activities states, "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning."[3]

Recommendation

Frequent monitoring over the backup process should be performed to ensure successful completion of data backup.

Management Response

DoIT concurs with this recommendation. Though there is monitoring in place - there is always room to improve our processes and procedures. The team will review all backup processes and procedures and enhance them, to ensure that ALL systems have an appropriate backup schedule in place, and that there are no lapses in documentation. This will be conducted by the end of this year (2017). DoIT is also currently evaluating multiple backup scenarios (disk-to-disk, disk-to-cloud, disk-to-disk-to-cloud) to improve the overall backup program. The final solution will include cloud based storage to replace onsite tape backups. This approach will resolve our most problematic disaster recovery challenges.

3. Backup Tapes Not Properly Secured and Infrequently Delivered to Storage Site

We observed backup tapes in an unsecured area of the DoIT office. Staff disclosed tapes were left there overnight pending preparation for the storage site. Although personnel entering the DoIT office must have authorized access, the backup tapes should be stored in a secured location to safeguard against loss or destruction. Additionally, DoIT personnel disclosed there are no regular scheduled deliveries of the tapes to the storage site. Best practice is that backup tapes should be timely transported to the storage site once retrieved from the data center to reduce the risk of loss or destruction of the tape and to ensure the availability of business critical data in the event of a disaster.

Recommendation

DoIT should ensure tapes retrieved from the data center are secured and delivered to the storage site in a timely manner to ensure availability of business critical data in the event of a disaster, and to reduce the risk of loss or destruction of backup data.

Management Response

DoIT concurs with this recommendation. Based on staffing levels, and the fact that personnel must perform multiple functions, it is not unreasonable to expect that tapes may

[3] Coso.org

not immediately be delivered to the secure storage site. As was noted in the review, the entire DoIT area is secured, and only authorized personnel have access, it is also reasonable to request that if staff cannot immediately deliver the tapes to the storage site, that they be placed in a secure area on premises. DoIT leadership has already mandated this because of the review, and has implemented this recommendation as of April 2017. It is important to note, all issues associated with physical tape management will be eliminated with the implementation of the disk-to-disk-to-cloud backup program, which we are targeting to have concluded, budget permitting, by the end of 2018.

4. IT Security Lack Direct Access to the Software Application Used to Help Safeguard Assets

IT Security does not have direct access to the software application used by Facilities Management (FM) to manage physical access to County owned and leased facilities, with the exception of Watershed and Sanitation Departments, as well as Judicial and Administrative towers. In addition, monitoring reports from the application are available to DoIT only upon request from FM. FM is responsible for adding or removing personnel physical access based on the department management's request.

The DoIT Physical Security Policy provides guidelines to help employees determine their accessible physical locations and with what level(s) of authorization. The policy also includes DoIT responsibility to monitor compliance with the policy. IT Security's limited access to the software application affects their ability for effectively monitoring non-compliance of the Physical Security Policy. Furthermore, IT Security provides an extra layer of oversight for monitoring the County's information systems and data and should have appropriate access to protect resources and ensure compliance.

Recommendation

DoIT should work with Facilities Management and the Sheriff's Office to obtain access to the physical security software and security reports to ensure compliance of the Physical Security Policy and to protect against unauthorized physical access to the County's information systems and data.

Management Response

DoIT concurs with this recommendation. DoIT has made numerous overtures to the previous leadership team of FM, but we were told that they would not restore access to the system because they felt that access control was the sole responsibility of FM. DoIT will work with the current leadership to obtain the level of access required to support operations and/or take over accountability and responsibility for operation and ownership of the entire system.

5. Limited Monitoring of Access Controls over User Accounts

DoIT is responsible for access controls for the County's Oracle System, Purchasing and Financial Management System, which includes adding or removing user access. In addition, they are also responsible for granting access and/or setting up user accounts for various other applications used throughout the County, as requested by user departments. However, if DoIT is not designated as the provider of security access over a system or application, they have no knowledge of access controls in place. System administrators and/or super-users in various County departments may perform functions that include access controls over the County systems and applications (e.g. Active Directory, PeopleSoft, etc.).

The following are examples of access control weaknesses:

- A review of a list of super-user accounts in Oracle identified users with access that should have been disabled. For instance, one user transferred to another division within the Finance Department and no longer required access to the Accounts Receivable module, but still had access. Another user had access to the Accounts Payable and Accounts Receivable modules, creating inadequate separation of duties. During the audit, DoIT modified the user accounts upon request from the department management. Internal Audit's inquiry into the issue revealed a department manager's uncertainty of the process for account modifications.
- DoIT utilizes a PeopleSoft interface in Oracle that notes terminated employees, as well as an employee termination and transfer report from PeopleSoft, to assist with disabling employee user accounts for those no longer requiring access. However, DoIT is not always aware when vendors no longer require access to a system or application, as they will not show up in the PeopleSoft data.
- In addition, DoIT disclosed some departments have the ability to use generic accounts in the Active Directory (e.g. Sheriff Department, Tax Commissioners, etc.), though some departments have set up password expiration controls. Such access creates a significant security risk and weakens monitoring and logging procedures; therefore, the system cannot track who made changes, which present accountability concerns.

"Access controls are the processes, rules and deployment mechanisms that control access, information systems, resources and physical access to premises."[4] They provide reasonable assurance that system assets are physically safeguarded and logical access to applications, system utilities, and data is granted only when authorized and appropriate. Without the DoIT knowledge of security access controls in place, there is the potential for unauthorized access by those looking to do harm (e.g. a disgruntled employee or vendor). In addition, awareness of access controls over systems and applications helps determine if controls are working as intended and helps to identify areas of improvements.

DoIT Information Security Policy states, "Directors(s) and other Department Leaders with support from IT are responsible for ensuring that information and information systems used within their areas of responsibility are managed and used in accordance with information security policies." In addition, the Utilization of Technologies Policy provides guidelines on protection against unauthorized access to the County's computer system; however, the policy does not provide direction to management on monitoring user access, especially those with super-user status or those created for vendors use. Furthermore, it does not provide guidance on the use of generic accounts and controls surrounding their use.

[4] ISACA®, "ISACA® Glossary of Terms," p. 1. 2015. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. (Assessed December 30, 2016)

Recommendation

IT policies should provide direction to department heads and system administrators on monitoring user accounts to ensure controls are in place that provides protection against unauthorized access. In addition, periodic monitoring should be performed over departments that rely on the department's own system administrators for security access controls over software applications.

DoIT should ensure departments requiring their services for security access controls over new applications are aware of DoIT process for account modification and acknowledge their understanding and agreement of the process.

Due to the risks associated with generic accounts, DoIT should work with department management to educate and provide guidance on the risks of generic accounts and IT controls.

Management Response

DoIT partially concurs with this recommendation. We wholeheartedly concur with the importance of user account management, and have implemented policies and procedures to support this requirement. We also concur that ensuring all individual system access is terminated upon their departure from county employ is a necessity. Having said this, we can control access to all systems by disabling access via Active Directory (AD). Though we clearly want all systems to have correct access control, if a system like Oracle or PeopleSoft is not immediately updated, it does not matter, as access will be prohibited/blocked because they cannot gain access once their AD credentials have been revoked. As a function of best practices, we will shore up procedures, and educate all staff to ensure that all application level credentials are current. DoIT fully concurs with the recommendation to conduct periodic monitoring of systems and applications that are under the purview of other department administrators.

6. No Configuration of Password Control in Oracle

Oracle's password lock-out feature is not enabled. In addition, the system is not configured for password expiration. A test was performed on the password reset feature and after more than three attempts to access the system, no lock-out occurred. A message alert repeatedly displayed, "after 3 attempts you will be locked out." Furthermore, there is the ability to immediately reuse the previous password. The DoIT disclosed there is no auto password expiration policy in Oracle that requires you to create a new password after a pre-set amount of time. Moreover, there is no policy to guide DoIT staff on password configuration requirements concerning application software. The IIA's *Auditing Application Controls* list an example of a password aging policy of every 90 days.[5] Password controls built into the Oracle system provide an additional layer of protection and is key to protecting financial data against unauthorized use or fraudulent activity.

[5] 90-Day Policy was taken from GTAG - 8: Auditing Application Controls, Institute of Internal Auditors, Altamont Springs, Fla., USA 2007

Recommendation

DoIT should work with the Oracle vendor to configure password controls for protection against unauthorized use. In addition, IT policy should include guidance on password configuration controls consistent with best practice.

Management Response

DoIT concurs with this recommendation. DoIT will research the feasibility of implementing a password expiration for E-Business Suite (EBS) and make updates to IT policy to reflect best practices.

7. Help Desk System Enhancement Needed

Persons requesting access to the Internet, remote-login, and Virtual Private Network (VPN) must submit a ticket through the DoIT Help Desk. The Manage Engine application is the help desk ticketing system used to document user requests. Yet, the application does not include a separate field to identify the person requiring Internet, remote, or VPN access. The "Name" field located in the "Requester Details" section of the application applies to the person inputting the request (e.g. supervisor, administrative assistant, etc.) and may not reflect the person receiving access, making it difficult to monitor for trends. Because the application is the source for documentation on user access, it is important that the application have the capability to monitor trends that may pose a risk to the County's information systems and data.

Recommendation

DoIT should explore options for enhancement of the Manage Engine application to include additional fields to allow the ability to monitor trends that can adequately assist in identifying abnormalities or discrepancies.

Management Response

DoIT concurs with this recommendation and will coordinate with the vendor to determine how this can be facilitated. DoIT will implement this feature as soon as it becomes available.

8. Control Weaknesses Identified in the Change Management Process

"IT Change Management can be defined as the set of processes executed within an organization's IT department designed to manage the enhancements, updates, incremental fixes, and patches to production systems, which include application code revisions, system upgrades, and infrastructure changes in the various stages of completion."[6]

The Business Solutions division is responsible for the change management process. They perform changes considered technical in nature (e.g. coding, configuration, upgrades, etc.). The division also may process functional changes (e.g. adding a field to a report) upon request from the user department.

[6] GTAG-2: Change and Patch Management: Critical for Organizational Success, Institute of Internal Auditors, Altamont Springs, Fla., USA 2012

We reviewed documentation for ten (10) regular and five (5) emergency change projects completed during the audit period. Below are examples of the findings:

- There was no supporting documentation to ensure segregation of duties *(DoIT staff making the change was not the same staff putting the change into production)*. DoIT disclosed there was no process in place to document segregation of duties during the audit period. Segregation of duties helps reduce the potential risk of errors or fraudulent activity. It ensures no one person has complete control over a transaction throughout its processing phase.
- There were no documented procedures of who was responsible for testing the change prior to approving the change for production. Per DoIT, if the change is a functional change (e.g. adding a field to a report), the user department is responsible for testing and notifying DoIT to move the change to production. DoIT indicated they rely on the user department for testing functional changes because DoIT staff may not always have knowledge of how the software application should work (e.g. functions performed in Oracle Purchasing and Contracting or Accounts Receivable modules).
- Several projects noted the user department initiated the change; however, there was no supporting documentation from the user department in the file. The DoIT relied on the helpdesk ticket number associated with the change project as support of user department request. In November 2015, the previous help desk application was replaced with a new application; however, the historical data was not transferred to the new system, leaving the DoIT with no historical data to confirm the change request.
- For one project, a department submitted a request to add security access groups to an existing application. Documentation of the request was inconsistent with the user departments. DoIT disclosed user departments are sometimes unaware of technical details for a change; therefore, DoIT communicates those additional needs.
- Some projects were missing key fields (e.g. originator of request, approving official's name and date approved).
- Approver names were keyed onto the project forms (electronic Word document) making it difficult to validate approval. In addition, in some instances there was no approval date.
- Several projects were noted as production changes; however, there was no supporting documentation to note user departments were aware of the change.
- Some of the project forms included an install date, which led one reviewing the document to conclude it referred to the installation date of the change. However, DoIT indicated the date served no purpose and because the form is a template, the current date may have been entered.

The Application Development and Installation Standard Operating Procedure (SOP) states, "Changes should not be installed without going through the proper procedures." In addition, the policy states, "Each change must be thoroughly documented utilizing Application Division standard templates and documentation guidelines." Lastly, the SOP states "Changes that do not adhere to documentation standard will not be installed in production." Management disclosed monitoring is performed on projects to ensure accuracy of the change.

Supporting documentation validates all party's involvement in the change management process, helps ensure documentation of approval and accuracy of changes, and that appropriate changes were made. Furthermore, documentation of the change management process provides an effective audit trail or research tool. Periodic monitoring of change management files can help detect areas of improvement.

Recommendation

User approval should be obtained for all revisions performed by DoIT to ensure changes are approved and consistency exists within the change management process.

In addition, the change management process should be monitored periodically to ensure controls are working that meet the goals and objectives of the process.

The following are some effective controls over documentation of the change management process to ensure project files include:

- Support of segregation of duties within the test and production environment
- Completion of all key fields on the project forms
- Supporting documentation of the user request for change
- Authenticated management approval and date
- Notice to user departments when production changes are made
- Clear identification of the party responsible for testing

Management Response

DoIT concurs with this recommendation, and has implemented some new internal procedures to address internal change management processes. Additional policy and procedure changes will be implemented based on best practices by year-end 2017.

9. Control Weaknesses identified in the Application Implementation and Upgrade Process

Most software applications implemented on the County's system are pre-packaged software products that cover a variety of business needs; thus, significantly reducing the need for in-house developed systems. "Advantages of purchased software are the rapid implementation, cost savings, and rigorous testing performed by the vendor prior to implementation at the customer's site."[7]

The Project Management Office (PMO) is responsible for initiation of projects involving IT infrastructure throughout the County. The PMO collaborate with other divisions within DoIT for completion of projects. The projects are documented in Daptiv, a software application used to manage projects and portfolios from start to finish. Some of its features include tracking with an option to document various tasks (Project Charter, installation testing, user sign, etc.) to assist in the project management process.

[7] Gilhooley, Ian. Information Systems Management, Control and Audit. Institute of Internal Auditors, 1991.

We focused on projects involving new system applications and upgrades to existing systems. The PMO submitted a Project Management Office Standard Operating Procedure policy (PMO-SOP) in draft form. Management indicated several of the guidelines would remain the same. We used the draft policy and interviews with management and staff as basis for criteria.

Documentation from seven (7) projects were reviewed with beginning or ending dates within January 1, 2015 to December 31, 2015 and were noted as closed in the PMO tracking system. Below are examples of the findings:

- The Project Charter form includes sections for the completion of the project schedule; preliminary risk assessment, assumptions and constraints; preliminary high-level budget; project resources; and approval. The approval section on the form was not filled out for two projects. In addition, five projects did not have a Project Charter form included in the file. The PMO indicated completion of the Project Charter depends on how a project was implemented; however, this is not outlined in the PMO-SOP. The PMO-SOP gives the definition of the project charter as "formally acknowledging that a project has approval to begin; and, that it is the authoritative document acknowledging the Projects' Executive Sponsor and the Business Sponsor signoff to initiate the project and the project manager acceptance to commence."
- Four projects did not have tasks identified in the Daptiv system.
- One project had various tasks listed (e.g. set/up configure IT Security, UAT Testing, User Training, etc.); however, it showed zero percent completion with no supporting documentation.
- One project showed end-user training; yet, there is no documentation to note all who attended the training.
- There was no documentation for all seven projects to support the completion of testing.

The PMO indicated the division at the time was going through a restructure and staff was being trained on processes.

Documenting the processes related to implementation and upgrade of software applications is important as it provides evidence of approval, testing to ensure successful implementation, end-user training, etc. In addition, lack of supporting documentation makes it difficult to monitor processes to determine where control weaknesses may exist and if processes are meeting goals and objectives of the PMO.

Recommendation

Documentation for projects involving implementation of application software and upgrades to existing systems should be completed, signed off by appropriate management, and properly filed in the tracking system to ensure evidence and completion of the project. In addition, periodic monitoring should be performed on project files to ensure the PMO process is working as intended.

To strengthen controls over the application implementation and upgrade process the DoIT should ensure the PMO-SOP policy draft is finalized.

Management Response

DoIT concurs with this recommendation, and has implemented new procedures that went into effect in March of 2017 to address this recommendation.

Comments

Penetration Tests

With cybersecurity effecting many organizations today, protective measures should be in place and effectively working to help reduce the risk of unauthorized access, fraudulent activity, and error in the County's information systems. DoIT should collaborate with department management on conducting penetration test that are reasonable, provide minimal disruption to County operations, and meet the purpose of the test. In addition, DoIT should engage an external source to perform an external penetration test of the County.

IT Steering Committee

The PMO receives requests for IT projects via telephone, email, or the IT Help Desk. As project requests are received, the PMO must obtain available resources, as their role of central IT support does not permit them authority to refuse projects. An IT Steering Committee (or equivalent) comprised of senior management and DoIT management may assist in prioritizing projects based on the County's overall objectives. ISACA defines an IT Steering Committee as "an executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects." [8] Cobit Control Objective PO4.3 – IT Steering Committee, contained within Process Define the IT Processes, Organisation and Relationships discusses an IT steering committee as including "business and IT participants to determine the prioritization of IT resources in line with business needs."[9]

Training for System Administrators

Since DoIT has central IT responsibilities, DoIT management should work with Human Resources (HR) department to explore mandatory training on IT risks and controls, including cybersecurity, for staff designated as system administrators throughout the County departments.

IT Security

As computer technology has advanced, our County have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Consequently, IT Security plays a critical/major role in safeguarding the County's information systems and data. The current job description of an IT Manager does not include language specific to include the duties of a person working in

[8] ISACA®, "ISACA® Glossary of Terms," p. 56. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. (Accessed December 30, 2016)

[9] http://www.isaca.org

the IT Security role. DoIT should work with HR to reassess the job description for staff performing the duties of an IT Security Manager.

Health Care Service Provider Contracts

The County exchanges sensitive health related data with Blue Cross Blue Shield (BCBS) and Aflac health service providers; however, during the audit there were no signed contractual agreements on file with the County for those organizations. In addition, a draft copy of an unsigned contract with BCBS obtained from Finance-Risk Management & Employee Services, did not include language about safeguarding County data. Yet, the contract did include language that a separate business associate agreement detailing BCBS's responsibilities regarding the Health Insurance Portability and Accountability Act (HIPAA) and the privacy and security regulations promulgated thereunder would be forthcoming. However, Risk Management & Employee Services did not have a business associate agreement on file.

With the emergence of the internet, new possibilities exist for widespread loss and abuse of personal, financial, and health information. Privacy, Data Security, and Data Breach Notification laws for health related information, such as HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH), provide protection for such information. Although these laws exist, implementing contractual controls provide wording that clearly delineate responsibilities and understanding of the potential liabilities.

Data Center Controls

DoIT is responsible for ensuring equipment that supports the business critical hardware in the data center is functioning and regularly maintained. However, FM maintenance records for the data center are forwarded to the DoIT only upon request. DoIT should work with FM to ensure all maintenance records regarding data centers are forwarded to DoIT as soon as the work is completed. DoIT should also ensure combustible materials in the data center are kept away from sensitive equipment, and stored to prevent injury to personnel and damage to mission critical data and equipment.

Mobile Devices

As a safeguard, DoIT performs data wiping on mobile devices for certain employees (e.g. Police, Sheriff) who report a County owned mobile device as stolen and file a report with the Police Services or Sheriff Department. DoIT should research options to provide this service to all to employees with a County owned mobile device that may report the device as stolen. There is a potential for sensitive County data to be stored on a mobile device as some devices provide storage ability. Data wiping all phones reported as stolen reduces the risk of sensitive data potentially being unlawfully obtained.

APPENDIX A – ACKNOWLEDGEMENTS

We would like to take this opportunity to thank the management and staff of DoIT, Facilities Management, Treasury, Risk Management & Employment Services, Records Management, Sheriff, and Police Services, for their assistance during this engagement.

Conducted by:

Camilla Cannon, CGAP
Senior Auditor
Finance Department - Internal Audit Division

Reviewed by:

Cornelia Louis
Deputy Director
Finance Department - Internal Audit Division

Lavois Campbell, CIA, CFE, CPA, CGA
Internal Auditor, Principal
Finance Department - Internal Audit Division

APPENDIX B – ENGAGEMENT OBJECTIVES AND SCOPE

Engagement Objectives

The overall objective of the audit is to assess general controls within the Department of Innovation and Technology's information technology.

The period covered is January 1, 2015 through December 31, 2015. The scope of the audit is to determine the following:

1. Access to programs and data is properly restricted to authorized individuals only.
2. All changes to existing systems are properly authorized, tested, approved, implemented, and documented.
3. New system/applications being developed or implemented are properly authorized, tested, approved, implemented, and documented.
4. IT supported system and programs/applications are available and processing accurately.

Engagement Scope and Approach

The audit did not include a review of the telecommunications component. Moreover, the business continuity component of IT general controls was addressed in an Emergency Management Review audit involving several key departments.

To meet the audit objectives, Internal Audit requested that DoIT complete an internal control self-assessment, interviewed management and staff, conducted site visits, observed and assessed processes, reviewed policies and procedures, and tested and reviewed available documentation.

APPENDIX C – DEFINITIONS AND ABBREVIATIONS

Divisions within Department of Innovation and Technology

Business Solutions Responsible for managing software applications for the County and ensuring operations are up and running.

Sub-divisions: Enterprise Resource Planning, Public Safety/Court Solutions, Enterprise Service Solutions, Database Administration Solutions, Change Management and Quality Control

Infrastructure & Operations Responsible for ensuring voice data, network, system storage, and helpdesk areas have the resources needed to accomplish daily tasks

Sub-divisions: Communication Technologies, Platform Technologies, and Enterprise Technology Center

IT Security Operations Responsible for maintaining integrity of information and resources, and for providing security, confidentiality, and availability of data

Strategic Support Responsible for strategic support and project management for installation of new applications and upgrades to existing systems, and other information technology related projects

Subdivisions: Administrative Operations, Project Management Office, and Business Alignment Support

Acronyms and Abbreviation

COBIT Control objective for information and related technology

COSO Committee of Sponsoring Organizations of the Treadway Commission

Key Definitions

Access Controls The processes, rules and deployment mechanisms that control access, information systems, resources and physical access to premises[10]

Application A computer program or set of programs that performs the processing of records for a specific function[11]

Backup Files, equipment, data and procedure available for use in the event of a failure or loss, if the originals are destroyed or out of service[12]

[10] ISACA®, "ISACA® Glossary of Terms," p. 1. 2015. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (Assessed December 30, 2016)

[11] Ibid., p. 4.

[12] Ibid., p. 11.

Business Continuity Preventing, mitigating and recovering from disruption[13]

Business Continuity Plan A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems[14]

Change Management A holistic and proactive approach to managing the transition from a current to a desired organization state, focusing specifically on the critical human or "soft" elements of change[15]

Cloud Computing Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[16]

Control The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature[17]

Data Wiping The process of logically removing data from a read/write medium so that it can no longer be read. Performed externally by physically connecting storage media to a hardware bulk-wiping device, or internally by booting a PC from a CD or network, it is a non-destructive process that enables the medium to be safely re-used without loss of storage capacity or leakage of data.[18]

Disaster Recovery Plan A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster[19]

Firewall A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between secure and an open environment such as the internet[20]

General Computer Control A control, other than an application control, that relates to the environment within which computers-based application systems are developed, maintained, and operated, and that is therefore applicable to all applications[21]

[13] ISACA®, "ISACA® Glossary of Terms," p. 14. 2015. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. (Assessed December 30, 2016)..
[14] Ibid.,
[15] Ibid., p. 18.
[16] Ibid., p. 20.
[17] Ibid., p. 26.
[18] http://www.gartner.com/it-glossary/data-wiping/
[19] ISACA®, "ISACA® Glossary of Terms," p. 34. 2015. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. (Assessed December 30, 2016).
[20] Ibid., p. 42.
[21] Ibid., p. 44.

Information Systems

The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies[22]

IT Steering Committee

An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects[23]

Network

A system of interconnected computers and the communication equipment used to connect them[24]

Operating System

A master control program that runs the computer and acts as a scheduler and traffic controller[25]

Project Charter

A formal acknowledgement that a project has approval to begin. It is an authoritative document acknowledging the Project's Executive Sponsor and the Business Sponsor signoff to initiate the projects and the project manager acceptance to commence.[26]

Recovery Testing

A test to check the system's ability to recover after a software or hardware failure[27]

Risk Assessment

A process used to identify and evaluate risk and its potential effects[28]

Virtual Private Network

A secure private network that uses the public telecommunications infrastructure to transmit data[29]

Vulnerability

A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events[30]

[22] ISACA®, "ISACA® Glossary of Terms," p. 50. 2015. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf. (Assessed December 30, 2016).
[23] Ibid., p. 56.
[24] Ibid., p. 63.
[25] Ibid., p. 66.
[26] DeKalb County Information Systems Technology Project Management Office Standard Operating Procedures. 6. September 18, 2013
[27] ISACA®, "ISACA® Glossary of Terms", p. 77. 2015, https://www.isaca.org?Knowledge-Center/Documents/Glossary/glossary.pdf. (Assessed December 30, 2016).
[28] Ibid., p. 81.
[29] Ibid., p. 99.
[30] Ibid., p. 100.

APPENDIX D – DISTRIBUTION LIST[31]

This report has been distributed to the following individuals:

DeKalb County Board of Commissioners

Michael L. Thurmond, Chief Executive Officer

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Dianne McNabb, Interim Chief Financial Officer

Preston Stephens, Interim Assistant Finance Director

Robert Akins, Treasurer

Larry Jacobs, Deputy Director of Finance - Risk Management & Employee Services

Clyde Stovall Interim Director, Facilities Management

[31] *Audit observations were discussed with DoIT management during the Exit Conference on December 22, 2016. Audit report revisions were placed on hold in February 2017 pending the completion of the annual Trust and Agency (T&A) audits that are part of the Comprehensive Annual Financial Report (CAFR), and transitioning of Finance-Internal Audit Division staff. During the interim, there were a few changes to elected officials and senior staff (e.g. Board of Commissioner, Chief Executive Officer, and Director of Facilities Management) whose names are now reflected in the distribution list.*