City Auditor’s Office

Information Technology Services Department Review

Report Issued: April 30, 2018

Audit Report No. # 18 N–1

Cape Coral
FLORIDA

TO: Mayor and Council Members

THRU: Andrea R. Butola, City Auditor

FROM: Timothy DiSano, Assistant City Auditor

DATE: April 30, 2018

SUBJECT: Information Technology Services Department Review

The City Auditor's Office has completed a review of various areas of internal/external controls, risks, and security affecting Information Technology Services (ITS) and how the department is addressing them.

We would like to commend ITS for being proactive in adopting the Critical Security Controls Initial Assessment Tool, having the initiative to perform an updated security assessment, and engaging a firm to perform a Telecom Billing audit which resulted in cost savings for the City. Assessing vulnerabilities and information security risks, and developing plans to address these risks within the City's information technology infrastructure is critical to ensuring that City operations run smoothly.

We would like to express our sincere appreciation to ITS management and staff for the courtesy, cooperation and proactive attitude extended to the team members during the review. If you have any questions or comments regarding this audit, please contact Tim DiSano at 242-3308 or Andrea Butola at 242-3380.

C: John Szerlag, City Manager
Michael Ilczyszyn, Assistant City Manager
Jay Murphy, Contract Business Manager
Dolores Menendez, City Attorney
Rebecca van Deutekom, City Clerk
Michelle Hoffman, ITS Director
Audit Committee

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The City Auditor's Office performed a review of various areas of internal/external controls, risk, and security affecting the Information Technology Services (ITS) Department and how the Department has been mitigating these risks. Over the course of the past several years, ITS has performed or had third parties perform the following reviews or assessments:

- Information Security Assessment, by Clifton Larson Allen (CLA), September 2013
- DR Data Security (DRDS), LLC
- Critical Security Controls (CSC) Initial Assessment Tool
- Payment Card Industry (PCI) Compliance review
- Digital City Survey Recognition
- CLA Financial Audit IT Review Procedures
- Completion of Citywide Risk assessments
- Florida Department of Law Enforcement (FDLE) Criminal Justice Information's System Audit (CJIS)
- Telecom Billing Audit

Based on our evaluation of the assessments and reviews completed, it appears ITS has an effective process in place to identify and address Information Technology (IT) risks that can affect the City. As a result of this review, we have identified areas for additional monitoring, and we plan to incorporate this as part of our annual audit planning process beginning in fiscal year 2019.

For details of our assessment of these areas see the Results section. For a summary of monitoring areas see the Resulting Actions section.

BACKGROUND

It is important that the City keeps pace with the ever-changing and sometimes complex world of IT to provide assurance that it is assessing internal/external controls, risk, and security in a timely and effective manner. While technology offers opportunities for improved communication, efficiency and effectiveness, it also represents threats, such as disruption, deception, theft, and fraud. IT controls are important to protect assets, customers, partners, and sensitive information. Controls must add value to the organization by reducing risk efficiently and increasing effectiveness.

Assessing and evaluating risk relative to IT can be complex. The IT infrastructure encompasses hardware, software, applications, data, procedures, and communications, as well as their operation within physical space, the organizational structure and its environment. Infrastructure also encompasses the people interacting with the physical and logical elements of systems.

ITS is responsible for delivering value, and providing information technology that supports the business needs of the City. ITS consists of five divisions: Business Applications, Geographical Information Services (GIS), Systems and Operations, Network and Telecom, and Security. The fiscal year 2018 adopted budget was $6,558,854. ITS has 26 employees when fully staffed.

Currently, the City and ITS have several risk mitigation strategies:

- Accept the risk
- Eliminate the risk
- Share the risk
- Control/mitigate the risk

OBJECTIVE

The review objectives were as follows:

- Determine if the City is adequately addressing IT risk.
- Determine if future ITS reviews or audits are necessary.

SCOPE AND METHODOLOGY

The review scope focused primarily on a review of reports, audits and risk assessments applicable to the ITS during fiscal years 2016, 2017 and 2018.

The following items were reviewed:

- DRDS, LLC Report
- Digital City Survey submission
- CLA Financial Audit IT Review Procedures
- ITS policies and procedures
- City Auditor’s Office Citywide Risk assessments completed for 2018
- CLA, Information Security Assessment
- Telecom Bill Audit
- FDLE CJIS Audit

In conjunction with the review of the reports noted above, the following resources and guidelines were referenced:

- Critical Security Controls Initial Assessment Tool
- PCI Data Security Standard
- CSC Initial Assessment Tool
- Global Technology Audit Guide (GTAG)

We reviewed the information in these documents as well as the status of any recommendations if applicable to determine if ITS has appropriate methodologies and mechanisms in place to support, adequately identify, evaluate and address IT threats.

STATEMENT ON NON-AUDIT SERVICES

We performed this engagement as non-audit services and it does not constitute an audit performed under Generally Accepted Government Auditing Standards (GAGAS).

RESULTS

DRDS, LLC completed during 2016 – DRDS used a combination of security testing tools and methodology, along with leveraging 20 years of industry expertise, to determine and validate the level of risk affecting the City's information systems. This new assessment was performed as a follow up to the CLA issued in September 2013 (see Information Security Assessment, by CLA). This assessment resulted in 17 new findings and recommendations, ranging from medium to high risk and associated cost for implementation. ITS indicated that all 17 recommendations have been remediated. The risk was accepted for one recommendation which related to an external product ITS does not control. The City Auditor's Office inquired with ITS to gain an understanding of what corrected action were taken regarding the seven high-risk findings. We believe ITS has appropriately addressed the recommendations and accepted the risk as appropriate. No further review is required.

PCI Compliance Data Security Standard. The PCI Security Standards Council is a global open body formed to develop, enhance, disseminate, and assist with the understanding of security standards for payment account security. Maintaining payment security is required for all entities that store, process or transmit cardholder data. PCI security standards provide guidance for maintaining payment security. These set of technical and operational requirements are for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

Payments for service are collected at various point of service (POS) terminals and applications throughout the City. Card numbers are not stored on any systems. The City has an internet-based software application used for E-Commerce, Cashiering, Web payments, POS and Hosted Payment Gateway.

Most of the City systems, networks and applications are currently PCI compliant, with just a few areas remaining which are currently in the process of getting upgraded card readers, as well as network changes. ITS contracted with a vendor to perform a PCI readiness review which includes a validation of controls, review of network segmentation plans and completion of the Self-Assessment Questionnaire. This is scheduled to be completed during the second or third quarter of fiscal year 2018 after the updates are complete. The PCI Data Security Standard Assessment (attestation of Compliance for Onsite Assessments – Service Providers) will also be completed by another third-party vendor annually. We believe the processes in place adequately address the risks of PCI non-compliance for the City.

Beginning with fiscal year 2019, the City Auditor's Office intends to monitor the results of these third-party PCI Assessments annually.

CSC Initial Assessment Tool: ITS uses the *CSC Initial Assessment Tool (The Tool)* created by the Center for Internet Security (CIS). According to the CIS, the purpose of this tool is to:

> *…provide organizations with a simple means of performing an initial assessment of their information assurance maturity level based on the on the controls defined by the Critical Security Controls and the Council on Cybersecurity.*

The Tool provides a series of 20 foundational and advanced cybersecurity actions, where most common attacks can be eliminated. The 20 CIS Controls include:

- Basic CIS Controls
- Foundational CIS Controls
- Organizational CIS Controls

The Tool calculates a maturity level aggregate score and an implementation percentage by control. ITS completed the assessment and as a result developed a multi-year plan to implement the recommendations associated with these controls. ITS' initial focus is on high-risk areas identified in the assessment. They are currently in year two of the multi-year implementation plan.

Beginning with fiscal year 2019, the City Auditor's Office intends to monitor the progress of implantation during the multi-year plan. This monitoring may include obtaining external expertise if deemed necessary.

Digital City Survey: The Center for Digital Government (CDG) is a national research and advisory institute on IT policies and best practices in state and local government. In November 2017, the CDG recognized the City with the top ranking for the category 125,000 to 249,999 population. The survey, which is open to all US Cities, assesses how our nation's municipalities are applying technologies to better serve their constituents and is considered a benching marking tool for state, city and government leaders. The 2017 survey focused the following Top 10 Characteristics of a Digital City:

- Open
- Mobile
- Engaged
- Collaborative
- Secure
- Staffed/Supported
- Connected
- Efficient
- Resilient
- Use of Innovation and Best Practices.

According to the Survey, “The City has aligned its IT efforts to support the City Strategic Plan”. As an example of this, in support of City economic development/redevelopment, ITS was pivotal in negotiations for an interlocal agreement with Lee County Department of Transportation to share and expand fiber conduit within the City. ITS designed a “Smart Cities” system that was included as part of the 47th Terrace streetscape project, as well as created a GIS layer to identify upcoming capital projects. In addition to the fiber conduit agreement, ITS has increased citizen awareness and actively marketed obtaining building permits online. This effort resulted in increased usage of the online system from twenty-three percent to seventy percent of applicants. Finally, ITS assisted in the creation of a system called Property Checkbook, which focuses on transparency and assists property owners to see the cost of government.

The new City ITS Director, hired in October 2015, is focused on security and transparency and recognizes the growing threat to IT systems. ITS created and filled a new position of IT Security Manager and is actively recruiting for a full-time security focused position. We believe the Digital City recognition demonstrates the high level of service ITS provides to the City because of the evaluation criteria applied to country wide participants.

CLA Financial Audit IT Review Procedures: Each year as part of testing conducted by CLA for the Comprehensive Annual Financial Report (CAFR) certain procedures are performed pertaining to ITS policies and procedures and ITS provides CLA information for analysis, as requested. According to CLA, for fiscal year 2017, there were no findings identified relating to ITS as a result of their test procedures.

Beginning in fiscal year 2019, the City Auditor’s Office intends to inquire annually with ITS and the external auditors regarding any IT CAFR findings and corrective action plans.

ITS Department policies and procedures: ITS has 91 policies and procedures and three IT Administrative Regulations (AR’s).

These policies and procedures and AR’s are continually reviewed and updated. During 2017, all 91 policies and procedures were converted from COBIT 4 framework to COBIT 5. According to ISACA (previously known as the Information Systems Audit and Control Association which now goes by its acronym only, and is an international professional association focused on IT governance):

> *COBIT 5 is the only business framework for the governance and management of enterprise IT. It incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems*.

Also, all the policies are reviewed, updated, and approved if necessary at least every two-years. This continual review and update is appropriate and demonstrates the department is properly monitoring policies and procedures and AR’s.

Beginning in fiscal year 2019, the City Auditor's Office intends to monitor the progress to ensure that all the policies and procedures and AR's are reviewed, updated, and approved if necessary at least every two-years.

City Auditor's Office Citywide Risk Assessment responses: ITS recently completed the Auditors Office citywide risk assessments for several of the ITS divisions; GIS, Networks, Security, Business Applications and System and Operations. Based on the responses to the risk assessments it appears overall divisions in ITS represent a moderate level of risk. We believe our monitoring of the department will be sufficient to identify areas of concern for further review.

Telecom Billing Audit: The Advocacy Telecom Group performed a Telecom Bill Audit, in February of 2018. The audit identified approximately $90,000 in potential saving through cancelation of unused lines, receiving government discounts and renegotiated rates. ITS is reviewing additional potential cost savings. The City has realized around $17,000 in annual savings so far. This is an example of a review that the City Auditor's Office could perform in the future as resources allow.

FDLE CJIS Audit: FDLE completed a CJIS audit in March of 2017. This audit is conducted every three years. The CJIS is a technical audit performed to ensure that the Police Department IT is operating in compliance with the agency's Criminal Justice User Agreement (CJUA) with the FDLE and version 5.5 of the Federal Bureau of Investigation Criminal Justice Information Security Policy (CSP). Compliance ensures that the proper controls are in place to safeguard the full lifecycle of data in the criminal justice system. The audit revealed two operating procedures that are out of compliance with the requirements of the CSP and CJUA. These procedures are updated and now are in compliance with the CSP and CJUA. We believe periodic reviews such as this reduce the risk of non-compliance in sensitive IT areas.

Information Security Assessment, by CLA, September 18, 2013. This assessment was a recommendation which originated from the fiscal year 2011 External Financial Audit. The assessment recommended the City periodically perform evaluations to identify potential areas of intrusion vulnerability in the City's IT systems. As a result, ITS and the City Auditor's Office sought proposals to perform assessments covering the following areas, Web Applications Testing (WAP), External Vulnerability Assessment Scan (EVA), and Internal Vulnerability Assessment Scan (IVA). When this report was issued there were 122 potential vulnerabilities, of these 46 were identified as high risk, 50 as medium risk, and 26 as low risk. At the time of this report, ITS staff began immediately to remediate these findings, placing priority on those identified as high risk. The ITS team was tasked with self-reporting on the progress and completion of identified risk mitigation actions.

ITS quickly addressed the implementation of most of these actions. According to a follow up issued by the City Auditor's Office on March 30, 2017, because of foundational changes to some of the IT systems, in 2015, it was determined that performing a new vulnerability assessment would be most appropriate for addressing those 42 items that remained. In October 2015, ITS leadership changed due to Director's retirement. The new ITS Director indicated that vulnerability assessments are an operational best practice and should be performed by ITS themselves on a regular and periodic basis to identify potential areas of intrusion vulnerability. In support of this best practice, the ITS Director engaged DRDS, LLC to perform a new security assessment, which was completed during 2016. Upon the completion of the DRDS, LLC review, the original remaining 42 open items are considered closed and the new findings issued by DRDS, LLC were addressed by ITS. (See DRDS, LLC information).

Global Technology Audit Guide (GTAG) As part of this assessment, the City Auditor's Office provided ITS with a copy of the Institute of Internal Auditors (IIA), GTAG Information Technology Risk and Controls Practice Guide. We tasked ITS with assessing current policies and procedures using guidelines in Section 5, Assessing IT – An Overview. This section identifies 17 questions to consider when evaluating the control environment and selecting a suitable set of controls. We consider the responses to the questions in the GTAG a tool to perform an initial risk assessment that will allow for more in-depth analysis in areas as deemed necessary. Many of the 17 questions are addressed in the adopted CSC Initial Assessment Tool, and ITS policies and procedures updates and/or incorporated into IT reviews or audits performed by third parties. Based on this information we believe there are no concerns in this area since they appear to be adequately addressed by ITS.

RESULTING ACTIONS

As a result of this review, we have identified these items listed below as areas for additional monitoring. We plan to incorporate this as part of the City Auditor's Office annual audit planning process beginning in fiscal year 2019.

PCI Compliance reviews: *The City Auditor's Office intends to monitor the results of these third-party PCI Assessments annually.*

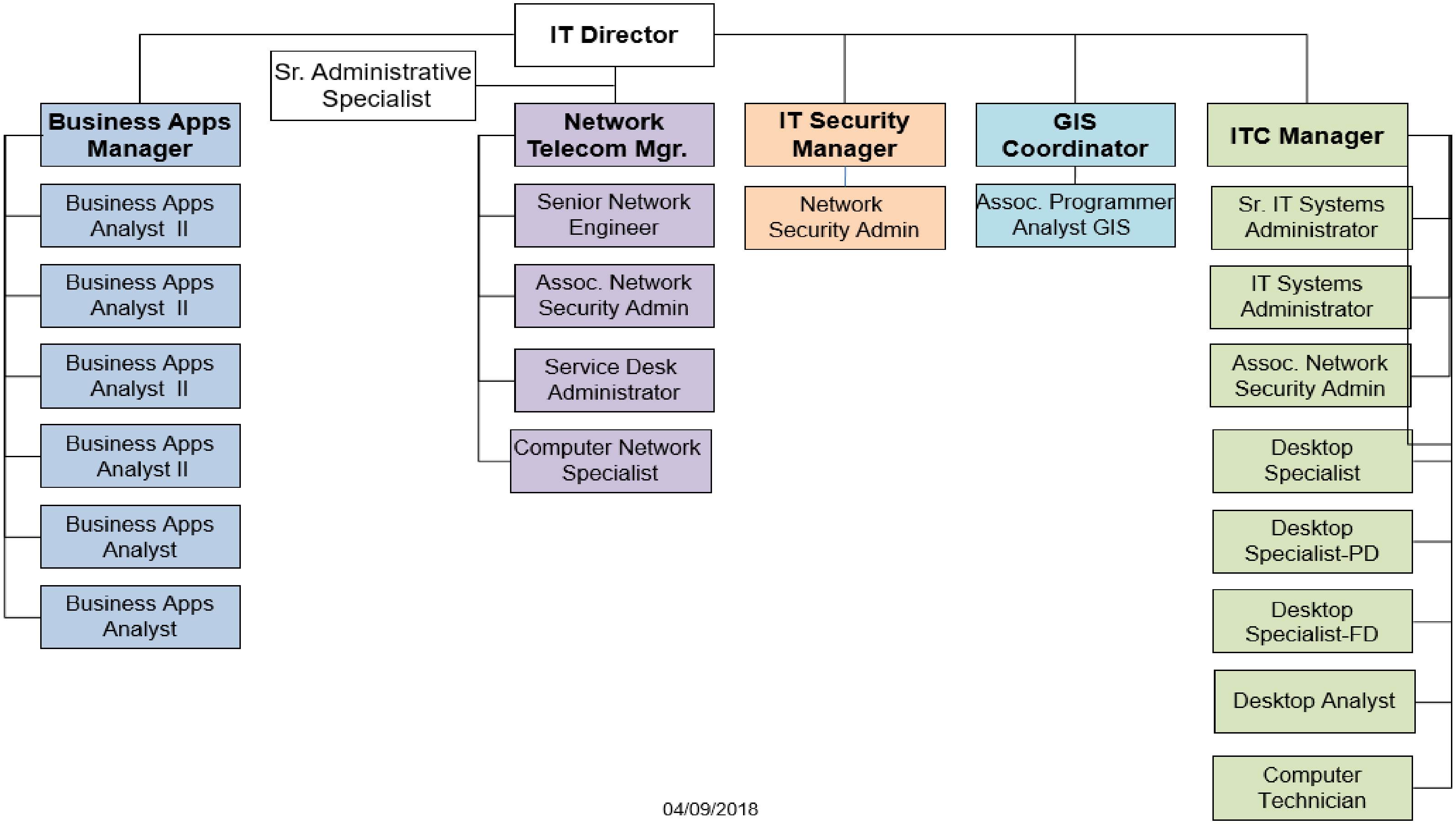
CSC Initial Assessment Tool review:
The City Auditor's Office intends to monitor the progress of implementation during the multi-year plan. This monitoring may include obtaining external expertise if deemed necessary.

CLA Annual CAFR IT review procedures
The City Auditor's Office intends to inquire annually with ITS and the external auditors regarding any IT CAFR findings and corrective action plans.

ITS Department policies and procedures
The City Auditor's Office intends monitor the progress to ensure that all the policies and procedures and AR's are reviewed, updated, and approved if necessary at least every two-years.

APPENDIX A

City of Cape Coral
IT Department Organization



04/09/2018