



OFFICE OF THE CITY AUDITOR AND CLERK

Date: May 4, 2012

To: Mayor Suzanne Atwell, Vice Mayor Terry Turner, Commissioner Paul Caragiulo, Commissioner Willie Shaw, and Commissioner Shannon Snyder

From: Pamela M. Nadalini, City Auditor and Clerk 

Subject: Sunera Audit Report of the Information Technology Department

Attached for your information and review is a redacted version of the above-mentioned detailed report. In accordance with Section 119.071(3), Florida Statutes, this report has been redacted to exclude items that identify current and past security vulnerabilities. If exposed, the security vulnerabilities that currently exist may pose a threat to the City's information technology infrastructure.

If you wish to discuss this report or have any questions, please do not hesitate to contact me at (941) 954-4169.

Attachment(s):

Sunera Report Project #CAC-2012-02, Assessment of Information Technology

c: Terry Lewis, Interim City Manager
Robert Fournier, City Attorney
John Jorgensen, The Sylint Group
William Culver, Manager, Information and Communication Technology
Heather Essa, MPA, CIA, CGAP, Manager, Internal Audit
File

RECEIVED

MAY 04 2012

City Auditor & Clerk



CITY OF SARASOTA

Assessment of Information Technology Department

Project: CAC-2012-02

This report is exempt from the Florida Sunshine Law in accordance with Florida § 119.071(3) due to the sensitive nature of the security plan information contained within. For questions please contact the City of Sarasota Attorney's Office.

January 2012

www.sunera.com

Table of Contents

Executive Summary	3
Objective.....	3
Scope	3
Approach	4
Technology Overview	4
Summary of Results	4
Summary of Recommendations	9
Detailed Results From Our Information Technology Assessment.....	15
IT Organization and Governance.....	15
IT Security	22
IT Operations.....	39
Recommendation Roadmap (“Security Plan”)	45
Project Plan	45
Appendices	49
Appendix A – Interviews Conducted.....	49
Appendix B – Current IT Organizational Chart	50
Appendix C – Recommended Policies and Guidelines.....	51
Appendix D – Assessment of IT by COBIT Process.....	53
Appendix E – COBIT Maturity Model for Internal Control	54

EXECUTIVE SUMMARY

The City of Sarasota ("the City") has engaged Sunera LLC ("Sunera") to perform an Information Technology (IT) Risk Assessment. Sunera is a leading provider of business consulting and technology risk management services throughout the United States and Canada. Our firm has performed numerous IT assessments of corporate, not-for-profit, and governmental organizations since its inception in 2005, and all resources for this project engagement hold highly-regarded industry certifications including Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and the Payment Card Industry's (PCI) Qualified Security Assessor (QSA) designation.

The City has requested this IT assessment to assess the controls that have been employed to ensure the integrity, availability, and confidentiality (where exempt from the State of Florida's public records "Sunshine Laws") of critical systems, data, and processes. This document, which is the resulting deliverable, may be used by the City to identify current state risks and prioritize the future initiatives required to reduce those risks. Due to the fact that this engagement was an assessment and not a financial audit, a formal sample methodology was not used.

Objective

Sunera was engaged by the City to perform an IT Risk Assessment in accordance with commonly applied, standard IT assessment frameworks. The Risk Assessment will enable the City to perform the following:

- Identify ways to better secure the IT systems that store, process, or transmit sensitive employee, taxpayer, resident, and cardholder information;
- Better ensure the integrity and availability of public information; and
- Enable City leaders, as stewards of taxpayer money, to make well-informed decisions regarding the level of risk associated with the current state of its IT systems and processes.

Scope

This assessment included the review of personnel, processes, and technology used by the City to conduct regular business operations and provide services to its taxpayers and residents. We focused our assessment on resources most critical to routine, daily operations, and the review was not restricted to any subset of systems or IT personnel maintained or employed by the City. It should be noted, however, that the City of Sarasota Police Department (SPD) maintains its own IT staff, and SPD IT systems and personnel were not included in the scope of this assessment. The assessment was performed on-site at the City of Sarasota, Florida during late November and early December 2011.

At the direction of the City, we performed an assessment of the following:

- IT governance and operations;
- IT organization and structure; and
- Current IT security processes, procedures, and infrastructure.

Approach

Sunera performed this assessment of the City's IT Department in accordance with select objectives defined using COBIT 4.1, ISO 27001, and the Payment Card Industry Data Security Standard ("PCI DSS") v2.0, international standard frameworks for conducting IT-related risk and security assessments. These frameworks provide risk-based, process-focused methodologies that we used to establish a thorough understanding of the City's objectives, the risks that threaten those objectives, and the relationships between those risks and the City's controls.

To conduct the assessment, we interviewed key IT personnel who were considered owners of the controls associated with each objective (interviewees are listed in Appendix A) on site from November 29 through December 2, 2011; inspected relevant policy and process documentation; and obtained and reviewed select operating system, network, and application configurations.

Technology Overview

The City's IT department is comprised of eight full-time employees and three contract employees, with one full-time position vacancy, who support approximately 500 workstations on one Windows domain – sarasotagov.net. (Appendix B provides an overview of the City's IT personnel organizational structure.) The majority of end user systems run the Windows XP Professional operating system; however, fewer than 10 workstations are piloting Windows 7 Enterprise. IT supports servers running Windows 2000, 2003, and 2008 and VMware ESXi 4.1. Critical systems and infrastructure are primarily hosted at the Sarasota Police Department's data center, with less critical and redundant systems hosted at the secondary data center located at City Hall.

Summary of Results

As a result of this assessment, we noted that the City's IT Department has managed to support its end users relatively well considering its limited resources, and performs extensive strategic and tactical planning to align with the objectives of the City. However, we also determined that the City currently maintains an IT infrastructure with significant security risks. The IT Department is understaffed, and City leaders and IT management have placed an emphasis on IT governance at the expense of a securely configured, high-availability network and systems. IT processes are at a low level of organizational maturity, as indicated by their *ad hoc* nature and lack of documented procedures and standards. An evaluation of the IT maturity level by COBIT process is provided in Appendix D. Specifically, we found the following issues to be potential inhibitors to the City's ability to ensure the security, integrity, and availability of its information systems. Although some of the identified issues impact many local governments, it is critical that the City ensures that resolution of these issues is a priority.

- **Alignment of IT.** During our assessment, we evaluated the fit of IT personnel within the Department as well as the alignment of information systems with business requirements and noted the following:
 - **Information Systems Alignment.** End users indicated that existing systems operate adequately to meet their daily job requirements, with limited exceptions. However, we noted that under the existing business model, disparate and antiquated applications are maintained by the City, with limited information sharing between applications. Each system requires its own specialized support knowledge and vendor support contract, which increases the cost of maintaining IT operations to the City.

- **IT Advisory Committee.** The City has established an IT advisory committee with representatives from key IT stakeholders, but the meetings are currently *ad hoc* in nature (e.g. no meeting minutes or agendas) and the stakeholders have limited decision-making authority.
 - **Service Hours.** The City Auditor and Clerk's Office maintains normal business hours of 8:00am to 5:00pm, Monday through Friday, which are also applicable to the IT Department. However, there is uncertainty within IT management as to the flexibility of this policy in providing service to meet end user needs.
- **IT Staffing Levels.** During our assessment of the IT organization, we noted that the City's IT Department was understaffed compared to governmental averages. Although current staffing levels have not impacted overall levels of service to end users, it has created knowledge silos in the areas of network administration, server administration, and telecommunications. In addition, the City uses a combination of contractors, application vendor support, and internal personnel to perform the database administration function, increasing the risk of inconsistently and inappropriately applied security configurations.
- **Evaluation of IT.** Monitoring qualitative and quantitative metrics pertaining to the performance of IT personnel, processes, and technology is critical to ensuring the security, availability, and integrity of information systems. We noted, however, that personnel performance evaluations for IT staff have been inconsistently performed. Additionally, key performance indicator (KPI) metrics used by management to evaluate IT operations are limited and provide an incomplete picture the IT Department's overall performance.
- **Formalized IT Documentation.** Although the IT Department maintains an IT policy set, several key IT policies have not been drafted, and the Computer Security Incident Response Plan has not been formally adopted. IT policies are not formally reviewed, updated as needed, and approved on an annual basis. Further, the City does not maintain formally documented network, server, and database security baseline documentation which define the minimum security requirements for information systems. Drafted network diagrams do not reflect the current state of the City's network architecture, and data flow diagrams, which outline the storage and transmission of critical data over the City's information system components, have not been created.

Enterprise Resource Planning (ERP) System Implementation Risks. We noted that during the ERP vendor selection process, the Utilities Department was not directly represented during the product demonstration process and final selection due to scheduling conflicts and the fact that an alternate representative was not selected at the outset of the selection process. This potentially increases the risk that the application does not fully or appropriately meet the needs of the Utilities Department end users. Further, the City does likely not have the internal project management and technical experience and capacity to permit effective implementation of the solution.

- **Payment Card Industry (PCI) Compliance.** The City is required to be compliant with the PCI DSS version 2.0 due to the fact that it accepts credit cards for payment as a merchant at locations including, but not limited to, the Van Wezel Performing Arts Hall (online and in-person), Bobby Jones Golf Course, and Robert L. Taylor Community Center (as of September 2011). The City completed PCI Self-Assessment Questionnaire 'C' ("SAQ-C") in

- [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
- [Redacted]

➤ **Server and Application Administrator Access.** During our assessment, we evaluated select server and application administrator access, and noted the following:

- [Redacted]
- [Redacted]

- [Redacted]
- [Redacted]

➤ **Windows Access.** During the assessment, we evaluated Windows user and workstations controls and noted the following:

- [Redacted]
- [Redacted]
- [Redacted]

➤ [Redacted]

[Redacted]

➤ **Document Retention.** E-mail messages transmitted using Microsoft Exchange Hosted Services (EHS) are stored for 30 days by EHS (i.e., "in the cloud") and are not captured by the City's Exchange server. Messages transmitted outbound from EHS bypass both the City's Exchange server and Quest Archive Manager, and are not retained by the City beyond 30 days which could put the city at risk of not being able to fulfill public records requests in violation of state open records statutes.

We also noted that when a new workstation or laptop is deployed, the contents of the 'My Documents' folder are stored locally on hard disk instead of being redirected to the user's network directory. As a result, there is an increased risk that documents are stored locally on the user's hard drive and not stored on the network file share which is backed up to tape and subject to forced record retention requirements.

- **Informal Service Level Agreements (SLAs).** Although the IT Department has created an internal SLA framework, it does not currently enter into binding SLAs with City departments. Overall, end users were satisfied with response and ability of IT support personnel, with limited exceptions. However, SLAs ensure that IT can be held to a reasonable standard that is agreeable to all stakeholders.
- **Security Awareness Training.** Security awareness training was prepared and presented to City employees in October 2010. However, attendance at the training was not mandatory or tracked. Security awareness training reinforces end user roles and responsibilities for information security and reduces the risk of social engineering attacks, whereby individuals are manipulated into divulging confidential information.
- **Disaster Recovery and Continuity.** The recently developed Continuity of Operations Planning (COOP) program has not been tested. We also noted that IT Disaster Recovery Plan procedures have not been fully documented and implemented.

Summary of Recommendations

As part of our procedures, we identified opportunities for improvement and documented the results in the detailed findings section of this report. To assist City leaders and IT management with prioritizing future remediation projects related to identified weaknesses, the following is a summary of key recommendations that should be considered for implementation by the City, as tax revenues permit:

- **Alignment of the IT Department.** In order to remediate the findings associated with our evaluation of IT personnel within the Department as well as the alignment of information systems with business requirements, the City should consider the following recommendations:
 - **Information Systems Alignment.** To alleviate the issue of disparate and antiquated applications with limited information sharing between them, the City should continue with its planned ERP implementation if it can be adequately staffed as discussed in the ERP System Implementation Risks section, below.
 - **IT Advisory Committee.** The City should formalize its IT Advisory Committee meetings by establishing a committee charter that establishes its decision-making authority. The committee should also document meeting agendas and minutes regarding discussions and decisions.
 - **Service Hours.** The City Auditor and Clerk should ensure that there is clarity and flexibility in internal City labor policies so that IT management has sufficient autonomy to schedule "exempt" IT personnel, who are designated as "on-call" for after hours support, or "non-exempt" personnel, who may be assigned to planned after-hours system maintenance, within the Department's defined policy framework.

- **IT Staffing Levels.** To address issues noted with the City's IT Department staffing levels, the City should consider hiring two full-time contractors assigned to the systems and network support group ("back-office support"), with an emphasis placed on cross-training and knowledge transfer. The City should also consider diverting the budget for its planned "Application Developer" to instead hire a database administrator (DBA). Database administration will become especially critical with the centralized storage of data with the City's planned ERP implementation.
- **Evaluation of IT.** To address findings related to the monitoring of metrics pertaining to the performance of IT personnel, processes, and technology, IT management should perform evaluations for all IT Department personnel on an annual basis to ensure that personnel are held accountable for their job performance. Additionally, IT management should augment its existing KPI metrics and ensure that a strong focus is placed not only on desktop support and budgeting but also on enterprise systems infrastructure and architecture.
- **Formalized IT Documentation.** During the assessment several weaknesses were noted regarding a lack of formalized IT documentation. To remediate these findings, the City should consider the following recommendations:
 - Ensure that a complete IT policy set is maintained to govern all critical City IT operations, consistent with best practices.
 - Ensure that all policies related to information security and IT operations are reviewed, revised as needed, and approved at least annually.
 - Review, approve, and formally adopt the Computer Security Incident Response Policy. On an annual basis, management should enact a test of the response policy and associated procedures to ensure that it is feasible and appropriate and that incident responders are familiar with the required steps.
 - Ensure that all network diagrams are updated to reflect the current state of the network architecture and ensure that data flow diagrams which overlay the network diagrams are created to depict the flow of critical data across information system components.
 - Document minimum security baselines for network devices, servers and databases.
- **Enterprise Resource Planning (ERP) System Implementation Risks.** The City should continue with its planned ERP implementation to enable a more efficient sharing and processing of information between departments. The size and scope of the project creates a significant risk with respect to successful project completion, and the project will likely be under external scrutiny. As such, the City Commission should ensure that City leaders, taxpayers, and stakeholders are provided with periodic and objective reports of project risks, combined with an assessment of the controls or methods planned or implemented to help mitigate the risk of project failure.

The City should also re-evaluate its internal processes whereby there is no provision for alternate representation in the event a primary vendor selection committee member is unable to attend all meetings and an alternate member is not in attendance from the commencement of the meetings. In any major project impacting multiple departments, full representation is critical to ensure the selected vendor matches the needs of all impacted users. In addition, the City should evaluate whether the Utilities Department was provided sufficient input in the vendor selection process from June through November 2011, with a focus on the product demonstration tasks of the ERP Selection Project, prior to sign-off on the final contract.

Further, while the intent of this assessment was not a comprehensive ERP project and skills review, during fieldwork we did identify that the current IT staff lacks project management (PM) capacity and skills. The individual (Manager Professional Business Services and an active employee during fieldwork) who holds a PM certification, was on administrative leave at the issuance of this updated report, does not have project management as one of her job responsibilities and likely does not have ample capacity to PM a project as effort intensive and complex as a major ERP implementation. Further, IT does not currently have the breadth or depth of technical experience that would be required for a major ERP implementation. As such, the City should consider hiring or contracting with a firm or resources who have sufficient knowledge and experience to perform the implementation.

- **PCI Compliance.** To ensure the City works toward compliance with all PCI DSS requirements, a comprehensive PCI gap assessment should be performed by a PCI Qualified Security Assessor (QSA) to identify all systems and business processes involved in the processing, transmission, or storage of cardholder data, as well as areas in which City is not compliant with the standard.
- **Network Security Management.** During our assessment, we evaluated the overall security of the City's network environment and noted several weaknesses as indicated in the Summary of Results section above. To remediate the noted issues the City should consider the following recommendations:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [Redacted text block]

- ☑ [Redacted text block]
- [Redacted text block]
- [Redacted text block]
- [Redacted text block]
- [Redacted text block]

- ☑ [Redacted text block]
- [Redacted text block]

- [REDACTED]
- [REDACTED]

➤ [REDACTED]

[REDACTED]

➤ **Document Retention.** The City should formally identify and document data retention periods for e-mail messages in an IT policy. Retention periods should be re-evaluated by the City Auditor and Clerk, City Attorney, and management annually to ensure that the City continues to meet legal standards and end user requirements. Additionally, the City should consider limiting the size of an individual's mailbox and periodically archiving e-mail messages, removing them from the Exchange environment. These archived messages should be retained in accordance with the aforementioned data retention periods in order to meet public records requests. To address the issue of e-mail messages transmitted outbound from EHS bypassing both the City's Exchange server and Quest Archive Manager, the City should implement and configure an e-mail solution that captures all messages to and from City personnel.

To ensure local workstation file retention, the City should automatically redirect, via Active Directory Group Policy Object, the 'My Documents' folder of each user to a network drive location specific to that user.

➤ **Service Level Agreements (SLAs).** IT management should define formal SLAs for services provided by the IT Department. The SLAs should be agreed upon, binding, and communicated between IT and the business process owners.

➤ **Security Awareness Training.** To reinforce end user roles and responsibilities for information security and reduce the risk of social engineering attacks, the City should implement a mandatory security awareness training program for all users of City information resources to be completed on an annual basis.

- **Disaster Recovery and Continuity.** IT management should continue to develop and implement detailed disaster recovery plans for IT. The City should also conduct an annual detailed test and evaluation of the Continuity of Operations Planning (COOP) Program plans and processes to ensure that they are updated regularly and key recovery personnel are trained on their responsibilities in the event of an actual disaster.

A Recommendation Roadmap complete with implementation timelines and suggested priorities is located on page 47 of this report.

DETAILED RESULTS FROM OUR INFORMATION TECHNOLOGY ASSESSMENT

The detailed findings and recommendations from our Information Technology Assessment are as follows:

IT Organization and Governance

IT Organization and Staffing

Organizational Risk: The IT Department is not organized, staffed, and managed appropriately resulting in undefined expectations of IT personnel, service and support delays, and an inefficient use of financial, personnel, and technological resources.

Impact – Moderate

Strengths

- ▲ **IT Department Internal Structure** – In early Q2 2009, the City reorganized the IT Department to contain two divisions – “Professional Services” and “Information and Communications Technology.” The “Professional Services” division manages projects and provides support to end users. The “Information and Communications Technology” division provides systems administration, implementation, and security services. The existing organizational structure appears to be sufficiently suited to support the IT requirements of the City.
- ▲ **IT Workload Planning** – Current workload planning is not based on formally documented planning schedules, but is flexible based on weekly requirements. This agility ensures that the IT Department can rapidly react to any support issues that occur during the course of normal operations. IT management plans for future staffing requirements when significant projects are on the agenda for the IT Department. For example, IT management has budgeted for an additional technical administrator and a business analyst for the planned ERP implementation, as would be expected for completion of such a large project.
- ▲ **IT Training and Skill Development** – The City IT Department has traditionally promoted career development by encouraging personnel to undergo training and pursue industry certifications. Certifications obtained by IT staff members include the CCNA – Security, CISM, A+, and Network+. In addition, the City leverages training provided by Microsoft as a part of its enterprise level licensing agreements. It should be noted, however, that there have been reductions in the training budget due to decreases in tax revenue in the overall City budget.

Weaknesses

- ▼ **IT Staffing Levels** – Due to budget constraints and attrition in recent years, the City has reduced IT staffing from 17 full time employees approximately four years ago to a present level of 12 employees. Based on recent IT staffing statistics¹ for the government sector, IT personnel average 5.6 percent of the total employee population. However, at the City, IT

¹ Michael Smith and Kurt Potter. *IT Spending and Staffing Report, 2009*. Gartner, 2009.

personnel are 2 percent of the total employee population, indicating that the IT Department is currently understaffed.

- ▼ **Knowledge Transfer and Single Points of Failure** – Reduced staffing levels, as indicated above, have resulted in concentrations of internal system configuration and support knowledge among few administrators at the City. Specifically, the systems administrator and network administrator represent two separate single points of failure where there are backups with only limited knowledge of internal system configurations. In the event of abrupt employment separations or staff paid time off, this may result in system support issues.

Recommendations

Although a significant number of IT personnel additions would be required to reach government sector averages, the City should consider hiring two full-time contractors as additional tax revenue becomes available in the future. The resources should be assigned to the systems and network support group ("back-office support") in the IT Department, with an emphasis placed on cross-training and knowledge transfer. The use of contractors would allow the City to maintain labor employment flexibility during precarious and changing economic conditions.

- ▼ **IT Service Hours** – Current IT support hours match the normal business hours of the City Auditor and Clerk's Office – 8:00am to 5:00pm, Monday through Friday. However, there are also City business functions that operate beyond normal business hours and occasionally require technical support, including, but not limited to, City Commission meetings, the Van Wezel Performing Arts Hall, Bobby Jones Golf Course, and Robert L. Taylor Community Center.

Under the existing policies of the City Auditor and Clerk's Office, as outlined in an intra-office memorandum dated October 21, 2011, "any time worked above and beyond the normal work day (i.e., overtime or comp-time) must be pre-approved prior to accruing the time." During interviews with IT personnel we noted that there is uncertainty within the IT department pertaining to the department's flexibility regarding scheduling and the ability to support end users after regular business hours.

Recommendation

The City Auditor and Clerk should ensure that there is clarity and flexibility in internal City labor policies so that IT management has sufficient autonomy to schedule "exempt" IT personnel, who are designated as "on-call" for after hours support, or "non-exempt" personnel, who may be assigned to planned after-hours system maintenance, within the Department's defined policy framework. The intent and understanding of the current policy should be reaffirmed with IT management to ensure clarity of the requirements.

- ▼ **Performance Evaluations** – During the assessment, we noted that although a mentor-mentee performance management model is in place, formal performance evaluations are performed on an *ad hoc* basis, with the most recent evaluations for IT personnel performed Q3-Q4 2009 or Q3 2010. The *ad hoc* nature of evaluations and goal setting may impede personal growth within City IT positions (i.e., human capital) and increases the risk that there is insufficient documented cause in the event that deteriorating work performance requires termination of employment.

Recommendation

Personnel evaluations should be performed for all IT Department personnel on an annual basis to ensure that personnel are held accountable for their job performance. A formal mechanism for goal setting and career development, as located on the last page of the City's "Employee Performance Evaluation" forms, should be used promote professional growth.

- ▼ **Alignment of Information Systems with Business Requirements** – Overall, business end users have indicated that critical applications used on a daily basis – including, but not limited to, FMS (Financials), Abra HR, Cartegraph, ESRI GIS, and Microsoft Exchange – meet their business requirements, with sufficient functionality and limited system downtime. However, under the existing business model, multiple disparate, and in some instances antiquated, applications that require specialized support knowledge and separate maintenance contracts are maintained by the City. In fact, the City's Permits, Code Enforcement, Local Business Tax Receipts, Contractor Registration, Billable Fees, TRIPS, and SCRAP applications reside on a version of Lotus Notes which is no longer supported. Additionally, significant silos exist whereby certain applications, such as Abra, FMS, and Cartegraph, have been historically managed and supported within business departments and not by IT administrators.

Recommendation

During the assessment, we noted that tax dollars were encumbered for the purpose of implementing an Enterprise Resource Planning (ERP) system, and the City was in the process of selecting a vendor. The selected ERP will provide a single platform for community development applications, utility billing, human resources, payroll, and financials. If implemented properly, the application modules will be integrated to enable a more efficient sharing of information between departments and increase efficiency by reducing the duplication of data entry.

- ▼ **Key Performance Indicator (KPI) Metrics** – An IT performance metrics spreadsheet was created by management for fiscal year 2010/2011 in response to the City's limited IT general controls audit dated June 10, 2009. Specifically, observation number four indicated that management should monitor the performance of IT operations. We obtained and inspected a copy of management's KPI spreadsheet and noted that it summarizes customer feedback from the use of the help desk, lists staff and budget meetings attended, and identifies whether budget amendments or fund transfers were requested. However, such KPIs do not adequately or effectively capture the enterprise level performance of IT.

Recommendation

IT management should re-evaluate its existing KPI metrics and ensure that a strong focus is placed not only on desktop support and budgeting but also on enterprise systems infrastructure and architecture. The existing KPI dashboard worksheet should be updated to encompass the following metrics, for example, for monitoring by management:

- Average systems availability and network downtime;
- Network utilization, quality of service, packet loss, and latency;
- Server utilization (i.e., RAM, CPU, and hard disk utilization thresholds);
- Timeliness of project completion;
- Overall project quality;

- Yearly IT spending by tower (e.g., hardware, software, support, communications, data center) compared to similar City IT Departments (i.e., benchmarking); and
- Percentage of attendance at critical IT meetings (e.g., status and committee meetings).

IT Policies

Organizational Risk: IT policies are not formally defined, leading to a lack of governance and the compromise of the confidentiality, integrity, and availability of information systems.

Impact – Moderate

Strengths

- ▲ **Acceptable Use Policy** – The City has implemented an end user acceptable use policy, in the form of a City Administrative Regulation, to govern the appropriate use of information systems. The policy addresses hardware, software, e-mail, Internet, and other IT equipment issued by the City for use in the workplace and states that violations of the policy may result in disciplinary action.
- ▲ **Communication of IT Policies** – The City IT Department publishes its internal policies to ePoint (SharePoint) to ensure that all relevant parties are aware of and have access to the documents. Additionally, administrative regulations, including the City's "Workplace E-mail, Internet, and Intranet Acceptable Use Policy," are published to eDocs to ensure that end users are aware of the City's workplace requirements.

Weaknesses

- ▼ **IT Policy Documentation** – During the assessment, we noted that there were a significant number of policies that were drafted and adopted by the IT Department. Existing policies include the following:
 - Information Security Awareness;
 - Information Security Policy Definitions;
 - Firewall Requirements;
 - Remote Access;
 - Default Accounts and Configurations;
 - Wireless Network Security;
 - Cardholder Data Security;
 - Vulnerability Management;
 - Anti-Virus, Anti-Malware, and Firewalls Policy; and
 - Secure Storage Room Policy.

However, we also noted that the City was missing policies that should be drafted and adopted, consistent with IT governance best practices, including the following:

- Logical Access;
- Change Management;
- Systems Development Lifecycle (focused more on systems implementation rather than actual development due to the limited development performed by the City's IT Department);
- Data Backup and Retention; and
- Help Desk Problem Management.

In addition, a Computer Security Incident Response Policy has been drafted but not yet approved and adopted.

Recommendation

IT management should ensure that a complete IT policy set is maintained to govern all critical City IT operations, consistent with best practices. Refer to Appendix C for details pertaining to the IT Policies and Guidelines that should be drafted and adopted by the City's IT Department. In addition, the City should review, approve, and adopt the draft Computer Security Incident Response Policy.

- ▼ **Annual Policy Review** – During the assessment, we noted that some IT policies had not been formally reviewed by IT management in over one year. Over time, policies may become less relevant to an organization due to changes in the risk landscape. Internal changes may include process changes, technology and system upgrades, and organizational structure changes. External changes may include regulatory or statutory restrictions and new security threats and vulnerabilities. A policy that no longer accurately pertains to the current organization will not effectively reduce the risks of that organization.

Recommendation

IT management should ensure policies related to information security are reviewed, revised as needed, and approved at least annually. The review and approval should be clearly evidenced either within the policy document or in ePoint. The revised and approved policies should be communicated and readily available to employees.

IT Planning

Organizational Risk: Short-term and long-term IT governance and planning are not performed, undermining the long-term direction of the City's IT Department.

Impact – Moderate

Strengths

- ▲ **Weekly IT Status Meetings** – During the interviews, we noted that the Director of IT holds weekly status meetings with the Manager of Information and Communication Technology, the Manager of Professional Business Services, and their respective teams to discuss IT operations, personnel management and staff workloads, significant system support issues, and project statuses. This ensures that daily operations of IT continue to meet the needs of the end users at the City.
- ▲ **Primary and Backup IT Support Personnel** – The IT Service Catalog maintained by the Manager, Professional Business Services lists all applications, functions, and services provided by IT in support of the City business operations. During the assessment, we noted that primary and secondary IT support personnel have been identified for key applications (e.g., FMS, Abra, Cartegraph, Granicus). It was also noted that the IT Service Catalog is currently undergoing revision and not all applications, functions and services have an assigned primary and secondary support person. Although the more critical applications and

services have been addressed, IT management should ensure that less critical applications are also assigned a primary and secondary support contact from IT.

Weaknesses

- ▼ **IT Advisory Committee** – The City has established an IT advisory committee with representatives from key IT stakeholders, including Finance, HR, Utilities, Public Works, Neighborhood and Development Services, IT, City Auditor and Clerk, City Manager, Van Wezel Performing Arts Hall, and Sarasota Police Department (for specific shared services only). Committee members meet at least annually to provide guidance and establish the technology direction for the City’s IT Department. However, the meetings are currently *ad hoc* with no meeting minutes or agendas. Stakeholder representatives have limited, if any, decision-making power.

Recommendation

The City should formalize the IT Advisory Committee meetings with an established committee charter, formal recurring meetings, and agendas and minutes regarding discussions and decisions.

- ▼ **ERP Selection Committee Process** – Although not expressly required by City Administrative Regulation Numbers 024.A007.0195 (“Purchasing Policies, Requirements, and Procedures”) or 024.A003.0194 (“Acquisition of Professional Services Procedures”), common practice at the City is to not provide for a replacement vendor selection committee member when an original committee member is unable to attend a significant number of meetings or meetings that are considered key to the selection process if the alternate attendee has not been identified at the outset of the selection process. The intent is to ensure that the alternate selection committee member does not make an ill-informed decision based on incomplete information from not having attended all meetings.

At the outset of the ERP vendor selection process, the following individuals were designated as representatives for key stakeholder departments:

- Sandra Coleman – IT;
- Gretchen Schneider – Neighborhood and Development Services;
- April Bryan – Human Resources;
- David Flatt – Financial Administration;
- Todd Kucharski – Public Works;
- William Mallett – City Auditor and Clerk; and
- Glenn Marzluf – Utilities.

However, in June 2011, Glenn Marzluf was eliminated from the selection committee meetings as he was unable to attend associated site visit meetings to view demonstrations of the ERP applications under review. Due to the fact that no alternate was selected for the Utilities representative at the commencement of the committee meetings, the Utilities Department was left without representation during the final months of the ERP selection process (June through November 2011). This increases the risk that the selected application does not appropriately and completely meet the requirements of the Utilities Department end users.

▶ [Redacted]
■ [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Recommendation
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

IT Security

Network Infrastructure Security

Organizational Risk [Redacted]
[Redacted]
[Redacted]
[Redacted]

Impact – High

Weaknesses

▼ [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Recommendation

[REDACTED]



[REDACTED]

Recommendation

[REDACTED]



[REDACTED]

Recommendation

[REDACTED]



[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

▼ [REDACTED]

▼ [REDACTED]

[REDACTED]

Recommendations

[REDACTED]

[REDACTED]

[REDACTED]

▼ [Redacted]

[Redacted]

[Redacted]

Recommendation

[Redacted]

▼ [Redacted]

Recommendation

[Redacted]

▼ [Redacted]

Note: Due to the sensitive nature of the security findings contained within the vulnerability scan report, please contact the City's Director, Information Technology for a full copy of the report findings.

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

Recommendation

The City's IT management should implement the recommendations identified within the external vulnerability assessment report. Findings designated as "Critical" or "High" should be remediated immediately. Findings with a "Medium" observation should be remediated as quickly as possible, but no later than one to three months from issuance of the report. "Low" observations should be remediated within six months to one year.

▼ [REDACTED]

Recommendation

[REDACTED]

▼ [REDACTED]

Recommendation

[REDACTED]

- ▼ [REDACTED]

Recommendation

[REDACTED]

- ▼ [REDACTED]

Recommendation

[REDACTED]

- ▼ **Computer Security Incident Response Plan** – IT management has drafted a Computer Security Incident Response that is consistent with industry best practices; however, the policy has not yet been approved and adopted by the City. As a result, there has not been a recent test of the City's Computer Security Incident Response capabilities.

Recommendation

IT management should review, approve, and formally adopt the Computer Security Incident Response Policy. On an annual basis, management should enact a test of the response policy and associated procedures to ensure that it is feasible and appropriate and that incident responders are familiar with the required steps. Performing a test of the response plan, including escalation, forensics capabilities or requirements, and reporting processes, will reduce errors and miscommunications that typically occur during an actual incident. Results of the test should be documented and include the capture of potential improvements along with any lessons learned.

▼ [Redacted text block]

Recommendation

[Redacted text block]

▼ [Redacted text block]

Recommendation

[Redacted text block]

- [Redacted list item]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Impact – High

Strengths

- ▲ **Secure Server Administration Protocols** – During our assessment, we noted that system administrators use Microsoft Remote Desktop Protocol for remote server administration. Through inquiry and observation we noted that the Remote Desktop Protocol encryption was set to “High”.

Weaknesses

▼ [Redacted text block]

Recommendation

[Redacted text block]

- [Redacted list item]

[Redacted text block]

▼ [Redacted text block]

[REDACTED]

Recommendation

[REDACTED]

▼ [REDACTED]

Recommendation

[REDACTED]

[REDACTED]

▼ [REDACTED]

Recommendation

[REDACTED]

[Redacted]

Application Security

Organizational Risk: Application vulnerabilities are undetected or not managed such that security measures are in line with business requirements leading to the compromise of system confidentiality, integrity, and availability.

Impact – Moderate

Weaknesses

- ▼ **Legacy Applications** – The City of Sarasota currently maintains Lotus Notes applications on a Windows 2000 server. In addition to Windows 2000 no longer being supported by Microsoft and the security vulnerabilities that exist, there is currently no one within the IT department with the knowledge and expertise to fully support the Lotus-based applications should issues arise.

Recommendation

The City of Sarasota should continue to move forward with plans to migrate business functions from the Lotus Notes application by implementing the selected ERP system and removing the legacy application from the production environment.

Patch Management

Organizational Risk: [Redacted]

Impact – High

Strengths

- ▲ **Windows Patch Management** – The City of Sarasota leverages Windows Server Update Services (WSUS) to patch servers and user workstations on a monthly basis. WSUS enables administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating systems. During interviews with system administrators, it was noted that prior to patches being pushed to all workstations and servers, they are first tested on test servers and training lab workstations to ensure system compatibility.

Weaknesses

- ▼ [Redacted]

Recommendation

[Redacted]



[Redacted]

Recommendation

[Redacted]

User Administration

Organizational Risk: [Redacted]

Impact – Moderate

Strengths

- ▲ **FMS Administrator Access** – During our assessment we noted that administration privileges for the FMS application is restricted to four individuals: [Redacted]

All are part of the Financial Administration department and access is appropriate based on job responsibility.

Weaknesses



[Redacted]

Recommendation

[Redacted]

- ▼ **Domain Administrator Access** – During our assessment we noted excessive and inappropriate membership within the “Domain Admins” Active Directory group. [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Recommendation

[Redacted]

Password Management

Organizational Risk [Redacted]

Impact – Moderate

Strengths

- ▲ **Windows Password Parameters** – The City of Sarasota requires each Windows user to maintain a password with at least eight characters which must meet complexity requirements (i.e., three of the following five categories: uppercase letters, lower case letters, numbers, special characters, and any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase). Users must change their passwords every 90 days, and

they cannot be changed to any of the previous four passwords selected. [REDACTED]

Weaknesses

▼ [REDACTED]

Recommendation

[REDACTED]

Anti-Virus Management

Organizational Risk: [REDACTED]

Impact – Moderate

Strengths

- ▲ **Centralized Anti-Virus Protection** – The City of Sarasota has implemented Microsoft Forefront Client Security which is a robust data protection tool identified as a niche player in Gartner’s “Magic Quadrant for Endpoint Protection Platforms.” During inquiry with management, we noted the following appropriate configurations:
 - Forefront receives definition and application updates via Windows Server Update Services (WSUS) automatically;
 - All Windows based workstations and laptops supported by the City have anti-virus software installed;
 - Weekly, full disk virus scans are scheduled for servers;
 - Daily “Quick Scans” are scheduled for all workstations and laptops;
 - Real-time scanning is enabled for the workstations, servers and laptops; and
 - Management can manually push updates to and perform scans of all workstations and servers connected to the network using the enterprise console in the event of infection.

Database Security and Administration

Organizational Risk: Application databases do not meet user requirements and expectations, and systems are insufficiently administered leading to a decrease in productivity and insufficient security of mission critical data.

Impact – Moderate

Strengths

- ▲ **Database Role Implementation** – The City’s database administrators have configured databases such that application accounts are not able to make modifications to the database schema or security parameters. End user accounts are constrained to specific actions and are not permitted to directly access data.

Weaknesses

- ▼ [Redacted]

Recommendation

IT management should migrate existing databases to a supported DBMS such as Microsoft SQL Server 2005 SP 3 and Microsoft SQL Server 2008 SP 1, or later. However, it should be noted that under current released schedules, Microsoft only plans to support SQL Server 2005 Service Pack 3 through January 10, 2012.

- ▼ **Inconsistent Database Administration** – The City relies on a combination of external contractors and internal resources for database systems support and administration which leads to inconsistent database configurations, security, and support. The skill set for effective database administration does not currently exist internally and the City would have to expend substantial resources to attempt to develop internal resources to perform database administration.

Recommendation

The City should consider diverting the budget for its planned “Application Developer” to hire a database administrator who would be responsible for the maintenance, administration, and secure development of databases, creation of database security standards and procedures, database backups, and overall support. Database administration will become especially critical with the centralized storage of data with the City’s planned ERP implementation.

- ▼ **Super User Account Password Access, Strength, and Modification** – During interviews with IT administrators, it was noted that the database administrator, or “super user,” account was used in some instances to logon to the database management console. The use of shared accounts, such as ‘sa’, increases the risk of repudiation for inappropriate actions, thereby reducing accountability for actions.

[Redacted]

[REDACTED]

Recommendation

[REDACTED]

Security Awareness

Organizational Risk: Users are not made aware of potential or current security risks leading to the compromise of sensitive data in hard copy format or electronically via the City's network and application infrastructure.

Impact – Moderate

Weaknesses

- ▼ **Information Security Awareness Training** – During our interviews with the City IT personnel, it was noted that in October 2010 security awareness training was prepared and presented to City employees; however, it was not mandatory for employees to attend the training. For those who did attend, verification of their acknowledgement and acceptance of the City's Information Security Policy was not documented.

Recommendation

The City of Sarasota should implement a security awareness training program for all users of City information resources to be completed on an annual basis. This training should be mandatory for all computer users and include, at a minimum, the following:

- A means by which the City can track the completion of the training.
- Key security information pertaining to the following subjects:
 - Information security responsibilities;
 - Protection of confidential data including cardholder data and PII;
 - Information system access controls and passwords;
 - Protection of mobile computing devices; and
 - Physical security controls.
- Required acknowledgement and acceptance by the user of the City's Information Security Policy.

Additionally, management should consider implementing additional security training throughout the year in the form of e-mail reminders, posters, or newsletters to keep personnel up-to-date with the changing security threat landscape.

Physical and Environmental Security

Organizational Risk: [REDACTED]

Impact – High

Strengths

- ▲ **Data Center Physical Security** – The City houses its critical servers and networking equipment at the SPD headquarters building on Adams Avenue in Sarasota in a data center that is shared with the SPD. The data center containing sensitive IT equipment is located on the 6th floor of a hurricane resistant building, constructed to withstand a Category 5 storm.

The City's equipment is located in a cage that is separate from SPD's equipment, with one doorway providing entry/exit access to the City of Sarasota's equipment. Access to the City's data center is restricted by a HID electronic badge system, with only City IT system administrator personnel and one SPD IT administrator permitted to enter caged area. Electronic badge access logs are maintained by SPD for 90 days.

[REDACTED]

- ▲ **Uninterruptable Power Supply** – Electricity to the data center is regulated by a Liebert nPower uninterruptable power supply (UPS) system. In the event the data center loses electricity over a longer period of time, the UPS devices would provide electricity to the data centers for less than one minute period of time required for the diesel-powered generator to initiate operation. A Kohler 1600kW diesel generator, model 1500REOZMB, is in place to provide backup electricity for the data center, including IT systems and HVAC equipment, for up to three days without refueling. The generator is tested monthly, with an annual test performed under load. Preventative maintenance is performed quarterly and the fuel storage system is inspected monthly.
- ▲ **Environmental Security** – The data center temperature and humidity is regulated by two independent, dedicated Liebert HVAC air handlers. The room temperature for the data center was configured to 70 degrees Fahrenheit. In the event the building loses power, the HVAC system would be powered by the generator, maintaining an appropriate room temperature. All equipment is positioned on a raised floor.

Smoke detectors are positioned throughout the data center, with visible and audible alarms located in the facility. An HFC-125 clean agent system has been implemented in the data center for automated fire suppression.

- ▲ **Visitor Access Register** – During our walkthrough of the City's data center at SPD headquarters, we noted that visitors were required to provide government issued identification and sign a visitor register upon entry to the facility. Visitors and vendors must be escorted throughout the building when on-site.

IT Operations

Application Performance and Availability

Organizational Risk: Applications do not meet end user performance expectations or become unavailable, leading to a decrease in productivity.

Impact – Moderate

Weaknesses

- ▼ **Archive Manager Performance** – During the assessment it was noted that the City of Sarasota currently has two instances of the Archive Manager application deployed. The “journal side” internal version of the Archive Manager application currently installed is version 4.1.2.434 and the public facing version of Archive Manager is 4.0.0.227. Neither of these versions are officially supported by the software vendor, Quest. The “journal side” captures all e-mails sent through the City’s Exchange server environment. A script within Archive Manager executes every hour to search the e-mail subject lines for “EXEMPT” (indicating the e-mail is exempt from public record) and removes it before copying the e-mails to the public facing Archive Manager instance. It is incumbent on the e-mail sender to correctly use and accurately spell the “EXEMPT” key word for Archive Manager to capture and remove such e-mails. During our interviews with City IT personnel, it was noted that the public facing Archive Manager is currently configured to search approximately 500 unique mailboxes; however, the application was not designed for such a task which is leading to some of the perceived performance issues.

Recommendation

The City of Sarasota should update to the most current version of the Archive Manager software so the vendor, Quest, will be able to provide support if necessary. To increase performance the City should consider limiting the number of mailboxes and amount of data the user can query on the public facing Archive Manager. Any e-mail communication older than a pre-determined retention period could be archived and provided by the IT Department upon request. An SLA between the IT Department and the City Auditor and Clerk could be established regarding IT fulfilling public records request and providing them on electronic media (e.g. CDs, DVDs, USB drives) to ensure requests are completed timely.

Additionally, the City should consider modifying the keyword EXEMPT to include special characters such as “[]” or “*”. This would help minimize errors related to e-mail messages incorrectly being removed from the public facing Archive Manager.

- ▼ **Exchange E-mail** – During our interviews with the City of Sarasota IT personnel it was noted that there is currently no size limitation on the users’ mailboxes. Additionally, an e-mail message is typically retained in a minimum of three separate locations: the users’ mailbox, the “journal side” Archive Manager and the public facing Archive Manager. Through inquiry with management, it was noted that there is approximately 2.4TB of e-mail already stored and this data store is growing at approximately 10GB per month. There is currently no data retention and disposal policy in place to define e-mail retention requirements and it is

currently the City's practice to keep all e-mail indefinitely from all current and past employees. The continual rapid increase of data being retained by the City has the potential to increase the cost associated with maintaining and searching the data as well as the performance and availability of the Exchange environment.

Recommendation

The City of Sarasota should formally identify and document data retention periods for e-mail messages based on statutory and regulatory requirements². Retention periods should be re-evaluated by management and legal counsel annually to ensure that the City continues to meet its data retention requirements. Additionally, the City should consider limiting the size of an individual's mailbox and periodically archiving e-mail messages, removing them from the Exchange environment. These archived messages should be retained in accordance with the aforementioned data retention periods in order to fulfill public records requests.

Problem Management

Organizational Risk: Problems and incidents are not resolved in a timely manner, and root causes are not investigated to prevent recurrence. Computing systems do not meet end user requirements leading to a decrease in productivity.

Impact – Low

Strengths

- ▲ **Computer Support Response Time** – During our interviews, City of Sarasota end users generally indicated that current response times to issues were meeting their expectations and requirements. As indicated by corroborative inquiry, overall, the end users complimented the IT department for their focus on customer service and responsiveness to requests for assistance.
- ▲ **Work Order Tracking and Prioritization** – The Computer Support team utilizes Numara Software's Track-It application, which is a robust help desk request and support tracking system, to enter, monitor, and resolve issues within the organization. We noted that all issues received by Computer Support team are routinely entered into the system. End users can call the dedicated support line, submit a request via the Track-It web portal, or submit a request via e-mail. If contacted by phone or e-mail, a Computer Support team member enters the ticket into Track-It. Additionally, internal SLAs are configured in Track-It to alert team members of approaching due dates and unresolved issues.
- ▲ **Use and Monitoring of Help Desk Performance Metrics** – Currently, the Manager of Professional Business Services oversees the performance of the Computer Support team. Reporting from the current Track-It system provides management with issue resolution metrics including customer satisfaction. On a monthly basis, a report showing the customer satisfaction survey responses is run to look for trends and monitor the resolution metrics of the Computer Support team.

² <http://dliis.dos.state.fl.us/barm/genschedules/GS1-SL.pdf>

Weaknesses

- ▼ **Service Level Agreements (SLA)** – The City IT Department does not currently enter into binding SLAs with the department stakeholders. During interviews with IT management it was noted that informal SLAs exist to track performance, but these have not been formally communicated to the business owners and are not binding. Without the use of SLAs, it is difficult to accurately and consistently measure the performance of the IT Department and take proactive measures to correct or improve inefficient or ineffective processes. Some City end users indicated that occasionally they or their staff members created Work Orders with the Computer Support team and never received notification from the appropriate parties of the problem resolution, creating ambiguity on the status of the request. As a result, although a solution may have been identified and implemented, a false sense of dissatisfaction may have developed among some end users.

Recommendation

Formal SLAs for services provided by the IT Department should be defined. The SLAs should be agreed upon, binding, and communicated between IT and the business process owners.

Formal or informal SLAs should address the following:

- Departments covered;
- Systems and networks covered;
- Process for service requests;
- Response levels (e.g. Critical, High, Medium, Scheduled, Project) with corresponding escalation procedures; and
- Service targets.

Additionally, before a ticket or issue is considered complete the Computer Support team member should always validate the resolution with the issue originator. This also reduces the risk that support personnel are closing tickets to meet internal SLA metrics without successfully remediating the issue. If there is going to be a delay in the resolution (i.e., additional research or awaiting vendor assistance) this should be communicated with the issue originator immediately. Continued use of the random end user satisfaction surveys will also assist in evaluating the SLA between IT and the business process owners.

System and Data Backups

Organizational Risk:

Impact – Moderate

Strengths

- ▲ **Data Backups** – The City of Sarasota has an established method for maintaining and protecting the organization's critical data. For overall management of backup procedures and monitoring, the City utilizes BackupExec 2010, a robust tool for performing backups. During inquiry with management, we noted that BackupExec performs and manage backups as follows:

- Daily incremental backups of production servers to disk are performed Monday through Thursday.
- Full backups of SQL databases are performed nightly.
- Weekly production backups to tape run Friday through Sunday.

For the servers judgmentally selected for inspection based on business criticality, including the FMS application and database, the Abra application server, the Lotus Notes server and the CSI server and database, we noted substantial completion of the backups, with the exception of open, and, therefore, locked files, as is common during backup processes. Note: tests of restoration were not performed within the scope of this assessment.

Weaknesses

- ▼ **Backup Tape Off-Site Storage** – During the assessment it was noted that backup tapes for the City’s critical systems in the SPD data center are currently stored at the City Hall data center. Although the maintenance of backup tapes off site is a sound practice, the close proximity of City Hall to SPD presents a risk of data being lost in an event that is more widespread, affecting both data centers. To augment this practice, the City of Sarasota should consider contracting with a 3rd party that is sufficiently far away (e.g., 50 miles) from either data center to maintain secure off-site storage of backup.

▼ [Redacted]

Recommendation

[Redacted]

▼ [Redacted]

Recommendation

[Redacted]

Disaster Recovery

Organizational Risk: Disaster Recovery Plans are not created and based on a formalized Business Impact Analysis that considers the impact of the loss of all essential functions, leading to increased down time in the event of a declared disaster.

Impact – High

Strengths

- ▲ **Continuity of Operations Plans** – In August of 2010, Calvin Giordano and Associates, Inc. (CGA) was retained by the City to conduct an evaluation of its Continuity of Operations Planning (COOP) Program. Subsequent to this assessment, in March 2011, CGA was retained to update and revise existing plans, including those for the IT Department. The Continuity of Operations Plans as they exist today were completed and provided to the City in June 2011. During the assessment we noted that the COOP has been formally documented and implemented for the IT Department. The following key elements of have been included as part of the plan:
 - **Activation Scenarios and Steps** – Guidance as to the detailed situations or conditions that would require COOP activation or the conditions under which a disaster should be declared "over."
 - **Business Impact Analysis** – Although a formally documented BIA was not performed, system criticality and priority was determined by the Director, Information Technology based on the feedback received from stakeholders. Each service item was assigned a score for Recovery Priorities, Business Function, and Recovery Time Objectives. The combined score represents the order services are to be restored by the IT Department for any disruptive event. The most current catalog with ranking scores is maintained with the Information Technology.
 - **Identification of Teams and Roles** – Designated members of the leadership team and recovery team members or their designated alternates have been defined.
 - **Recovery Time Objectives (RTOs)** – The RTO is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid the consequences associated with a break in business continuity. RTOs have been defined by the City as the following: 1 – Immediate; 2 – Within 6 hours; 3 – Within 12 hours; 4 – Within 24 hours; 5 – After all others
 - **Mission Essential Functions** – Prioritized agency functions that must be performed under all operational conditions have been identified. The COOP was created to ensure that these functions can continue to be performed even following a major disaster.

Weaknesses

- ▼ **Disaster Recovery Plan Procedures** – During the assessment we noted that the detailed IT disaster recovery plans (DRPs) have not yet been fully documented and implemented. DRPs provide preplanned activities or actions that reduce impromptu decision making during the recovery process and enable the resumption of normal operations in the most cost effective manner possible.

Recommendation

IT management should continue to develop and implement detailed disaster recovery plans for Information Technology. The City IT Department should ensure that the detailed disaster recovery plans include documented work steps identifying the activities required to restore access to critical systems, as well as network access. The work steps should also indicate how and from which vendors the recovery team should procure replacement server, client, and printer hardware.

In addition, the City IT Department must ensure that, when completed, the DRP is available in electronic and hard copy format in secured locations to ensure the information remains confidential, is handled appropriately, and is readily available in the event of a disaster.

- ▼ **Annual COOP Testing** – There has been no communication or initiative to perform annual testing (e.g., tabletop exercises) of the recently developed departmental COOP plans. Additionally, each department has their own departmental COOP plan and is solely responsible for any updates and testing.

Recommendation

The City should conduct an annual detailed test and evaluation of the plans and processes to ensure that they are updated regularly and key recovery personnel are trained on their responsibilities in the event of an actual disaster. Annual testing of the plans and processes will ensure the interdependencies among departments is also addressed and accounted for. Additionally, the role and responsibility of ensuring that all departments are maintaining and updating their plans annually should be defined and assigned to an individual. This individual should also act as the coordinator and liaison for the annual testing of plans.

RECOMMENDATION ROADMAP (“SECURITY PLAN”)

Based on the issues and recommendations identified in the IT Assessment, the City should plan to undergo defined remediation efforts. Accordingly, related recommendations have been logically grouped and categorized for project planning purposes in terms of priority (High, Medium, and Low) with regard to the recommended implementation timeline. The numbers associated with each remediation effort relate to items in the project plan, below.

	0 – 6 Months Phase 1	6 – 12 Months Phase 2	12 – 18 Months Phase 3
Higher Priority	<p>10. Evaluate whether the Utilities department was provided sufficient input in the ERP Selection Project prior to sign-off on the final contract.</p> <p>5. Continue forward with the proposed implementation of an Enterprise Resource Planning (ERP) system with appropriate resources.</p> <p>36. Remove public access to view e-mail via the web using Active Directory credentials.</p> <p>35. Re-evaluate use of Active Directory Domain Users accounts for media access to City e-mail.</p> <p>3. Ensure clarity and flexibility in Internal City labor policies so that IT management has sufficient autonomy to schedule personnel within the Department's defined policy framework.</p> <p>59. Re-evaluate the Exchange Hosted Services Archive Viewer configuration and implement a solution ensure all messages to and from City personnel are captured.</p>		<p>8. Review, revise as needed, and approve information security and IT operational policies at least annually.</p> <p>7. Draft, approve and adopt additional IT policies consistent with IT governance best practices.</p> <p>29. Review, approve, and formally adopt the Computer Security Incident Response Policy.</p>
		<p>23. Implement a vulnerability management process as well as perform internal vulnerability scans on a quarterly basis.</p>	<p>47. Consider diverting the budget for the planned "Application Developer" to hire a database administrator. Database administration will become especially critical with the centralized storage of data with the City's planned ERP implementation.</p> <p>50. Implement a security awareness training program to be completed on an annual basis.</p> <p>9. Re-evaluate internal processes regarding selection committee membership and provisions for alternate representation.</p>
		<p>22. Consider leveraging an external security firm to perform a detailed, independent network ACL and configuration assessment.</p> <p>25. Perform an internal and external penetration test on an annual basis.</p> <p>1. Hire two full-time contractors to be assigned to the systems and network support group ("back-office support") in the IT Department and increase emphasis on cross-training and knowledge transfer within the IT Department.</p>	<p>55. Identify and document data retention periods for online e-mail messages.</p> <p>53. Consider limiting the amount of data the user can search through on the public facing Archive Manager.</p> <p>4. Perform annual personnel evaluations for all IT Department personnel.</p> <p>62. Conduct an annual test and evaluation of recovery and continuity plans and processes.</p> <p>61. Consider contracting with a 3rd party to maintain secure off-site storage of backup tapes.</p>
		<p>56. Consider limiting the size of an individual's mailbox and periodically archiving e-mail messages, removing them from the Exchange environment.</p>	<p>57. Define minimum Service Level Agreements (SLAs) between the IT Department and business process owners.</p> <p>63. Assign an individual the responsibility to ensure all departments are maintaining and updating their COOP and detailed disaster recovery plans annually.</p> <p>54. Consider modifying the keyword EXEMPT to include special characters.</p> <p>13. Formalize the IT Advisory Committee meetings and consider including civic leaders as part of the committee.</p> <p>51. Implement a centralized audit logging solution.</p>
	<p>38. Develop an SLA between IT and CAC to provide requested records on electronic media.</p> <p>12. Ensure that a comprehensive PCI gap assessment is performed by a PCI Qualified Security Assessor (QSA).</p>		
Lower Priority	<p>58. Improve communication with end user regarding issue status and resolution.</p>		

Project Plan

This project plan outlines the action items by area and the phase in which the action should be completed.

PROJECT PLAN - Page 1

#	Recommended Action Item	Phase		
		1	2	3
IT Organization and Governance				
1	Hire two full-time contractors to be assigned to the systems and network support group ("back-office support") in the IT Department and increase emphasis on cross-training and knowledge transfer		■	
3	Ensure clarity and flexibility in internal City labor policies so that IT management has sufficient autonomy to schedule personnel within the Department's defined policy framework.	■		
4	Perform annual personnel evaluations for all IT Department personnel.			■
5	Continue forward with the proposed implementation of an Enterprise Resource Planning (ERP) system with appropriate resources.	■		
6	Re-evaluate and update existing KPI metrics.		■	
7	Draft, approve and adopt additional IT policies consistent with IT governance best practices.			■
8	Review, revise as needed, and approve information security and IT operational policies at least annually.			■
9	Re-evaluate internal processes regarding selection committee membership and provisions for alternate representation.			■
10	Evaluate whether the Utilities department was provided sufficient input in the ERP Selection Project prior to sign-off on the final contract	■		
12	Ensure that a comprehensive PCI gap assessment is performed by a PCI Qualified Security Assessor (QSA).	■		
13	Formalize the IT Advisory Committee meetings by implementing a charter and granting decision-making authority.			■
IT Security				
14		■		
15		■		
16		■		
17			■	
18			■	
19		■		
20			■	
21				■
22	Consider leveraging an external security firm to perform a detailed, independent network ACL and configuration assessment.		■	
23	Implement a vulnerability management process as well as perform internal vulnerability scans on a quarterly basis.		■	

Note: Numbers 2 and 11 were purposefully excluded as they were no longer required based on updates to report content made during the management review process.

PROJECT PLAN - Page 2

#	Recommended Action Item	Phase		
		1	2	3
24	Implement the recommendations identified within the external vulnerability assessment report.	■		
25	Perform an internal and external penetration test on an annual basis.		■	
26		■		
27			■	
28		■		
29	Review, approve, and formally adopt the Computer Security Incident Response Policy.			■
30		■		
31				■
32				■
33		■		
34			■	
35		■		
36		■		
37		■		
38	Develop an SLA between IT and CAC to provide requested records on electronic media.	■		
39	Document minimum security baselines for servers running a Windows operating system.		■	
40		■		
41			■	
42			■	
43		■		
44			■	
45		■		
46		■		
47	Consider diverting the budget for the planned "Application Developer" to hire a database administrator. Database administration will become especially critical with the centralized storage of data with the City's planned ERP implementation.			■
48	Migrate existing databases to vendor supported versions.		■	
49		■		
50	Implement a security awareness training program to be completed on an annual basis.			■
51	Implement a centralized audit logging solution.			■

PROJECT PLAN - Page 3

#	Recommended Action Item	Phase		
		1	2	3
IT Operations				
52		■		
53	Consider limiting the amount of data the user can search through on the public facing Archive Manager.			■
54	Consider modifying the keyword EXEMPT to include special characters.			■
55	Identify and document data retention periods for online e-mail messages.			■
56	Consider limiting the size of an individual's mailbox and periodically archiving e-mail messages, removing them from the Exchange environment.		■	
57	Define minimum Service Level Agreements (SLAs) between the IT Department and business process owners.			■
58	Improve communication with end user regarding issue status and resolution.	■		
59	Re-evaluate the Exchange Hosted Services Archive Viewer configuration and implement a solution ensure all messages to and from City personnel are captured.	■		
60				■
61	Consider contracting with a 3rd party to maintain secure off-site storage of backup tapes.			■
62	Conduct an annual test and evaluation of recovery and continuity plans and processes.			■
63	Assign an individual the responsibility to ensure all departments are maintaining and updating their COOP and detailed disaster recovery plans annually.			■

APPENDICES

Appendix A – Interviews Conducted

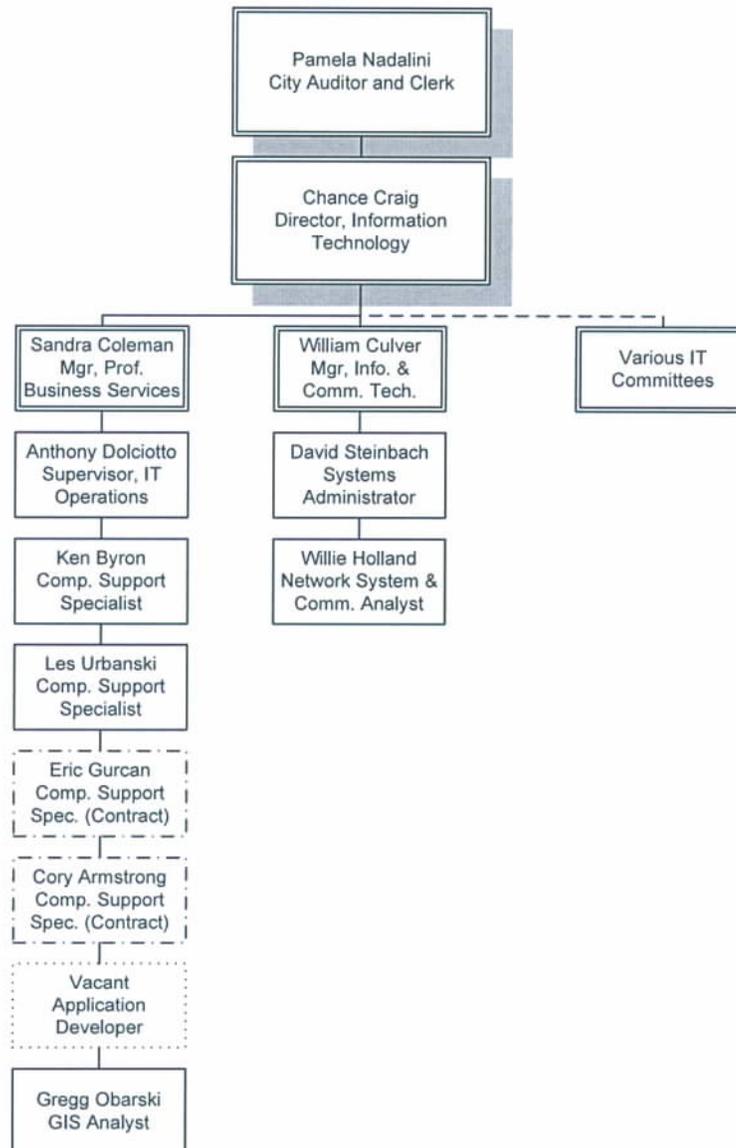
Below is a listing of all individuals interviewed to obtain the information for this IT Assessment:

Interviewee	Job Title
Cory Armstrong	Computer Support Specialist
Ken Byron	Computer Support Specialist
Sandy Coleman	Manager, Professional Business Services
Janice Cox	Process Improvement Specialist
Chance Craig	Director, Information Technology
William Culver	Manager, Information & Communications Technology
Cynthia Cumbie	Manager, City Records
Anthony Dolciotto	Supervisor, IT Operations
Heather Essa	Manager, Internal Audit
David Flatt	Manager, Accounting and Payroll Systems
Dolly Gamble	Supervisor, Accounting and Payroll Systems
Eric Gurcan	Computer Support Specialist
Willie Holland	Network System & Data Communications Analyst
Doug Jeffcoat	Director, Public Works
Kandy Lee	Administrative Assistant
William Mallett	Coordinator, Web Communications
Stacie Mason	Manager, Human Resources – Compensation, Benefits, & Risk
Karen McGowan	Deputy City Auditor & Clerk
Pamela Nadalini	City Auditor & Clerk
Paul Nelson	Microsoft Support Services
Mark Nicholas	Manager, Public Works Finance & Administration
Gregg Obarski	GIS Analyst
Nicole Olsen	Supervisor, Recreation Facilities
Adam Richter	Manager, IT – Sarasota Police Department
Lori Rivers	Deputy City Auditor & Clerk, Administrative Operations
Gretchen Schneider	GM Planning & Development
David Steinbach	Computer Systems Administrator
Mark Stinson	Accounting System Administrator
Linda Strange	Senior Planning Tech
Diane Torres	Administrative Specialist III – Commission Reporter
Les Urbanski	Computer Support Specialist

Appendix B – Current IT Organizational Chart

Office of the City Auditor & Clerk

Information Technology Department – City of Sarasota
December 2011



Appendix C – Recommended Policies and Guidelines

Recommended Document	Purpose	Topics Addressed
<i>Database Security Baselines</i>	Database security configuration baselines define the minimum security baselines for the City's databases.	Database security baseline documentation should include the following: <ul style="list-style-type: none"> ▪ database version and patch level; ▪ database instances and sizing; ▪ users assigned to administrator level server and database roles; ▪ accounts permitted to access the database directly; ▪ audit trail configuration; ▪ 'sa' password strength and change frequency; ▪ status of the 'guest' account; and ▪ services to be disabled.
<i>Server Security Baselines</i>	Server security configuration baselines define the minimum security requirements for the City's servers	Server security baseline documentation should include the following: <ul style="list-style-type: none"> ▪ disabling of non-essential services; ▪ removal or disabling of non-essential accounts (as required by the Default Accounts and Configurations Policy); ▪ modifying default account passwords (as required by the Default Accounts and Configurations Policy); ▪ file and directory protection; ▪ disabling file sharing, where applicable; and ▪ logging requirements.
<i>Network Security Baselines</i>	Network security baselines define the minimum security configurations for the City's network devices, such as firewalls and routers.	Network device baseline documentation should include the following: <ul style="list-style-type: none"> ▪ updating hardware and software; ▪ ensuring strong local passwords are implemented; ▪ disabling and/or removing unnecessary protocols and services; ▪ blocking unneeded ports; and ▪ ensuring appropriate use of ACLs to restrict traffic to only that required for business operations.
<i>Logical Access Policy</i>	Defines how to maintain an adequate level of security to protect data and information systems from unauthorized access	The following should be documented with respect to logical access: <ul style="list-style-type: none"> ▪ password requirements; ▪ access for non-employees; ▪ periodic access reviews; ▪ access approval; and ▪ change and revocation.
<i>Change Management Policy</i>	A document addressing change management to provide a structure for requesting, approving,	The following stages of the change management process should be addressed: <ul style="list-style-type: none"> ▪ change request; ▪ change request evaluation;

Recommended Document	Purpose	Topics Addressed
	testing and implementing changes to IT resources.	<ul style="list-style-type: none"> ▪ change specification; ▪ design specification; ▪ quality assurance; ▪ execution; ▪ testing; ▪ implementation; ▪ post-implementation analysis; and ▪ emergency change process.
<i>Systems Development Life Cycle</i>	A document which creates a formal approach to implement quality systems.	<p>The SDLC should incorporate the following stages:</p> <ul style="list-style-type: none"> ▪ feasibility study; ▪ analysis; ▪ implementation; ▪ testing; ▪ evaluation; and ▪ maintenance. <p><i>Note:</i> design and development does not currently apply to the City as application code is not developed by the City.</p>
<i>Backup and Retention Policy</i>	The purpose of this policy is to ensure the successful completion of server backups and retention of those backups to guarantee recovery of critical data in the event of a disaster.	<p>The backup and retention policy should include the following:</p> <ul style="list-style-type: none"> ▪ requirement to maintain a plan which explicitly specifies the servers to be backed up, the method of back up (e.g. to tape and/or disk), and the type of backup (daily full, weekly full, daily incremental, etc.); ▪ requirement to maintain a plan to retain backed up data in accordance with guidance from business users, the City Auditor and Clerk, and the City Attorney; ▪ requirement to maintain a plan detailing off site tape rotation; and ▪ requirement to perform regular testing of the validity of backed up data via restore.
<i>Help Desk Policy</i>	Establishes the scope and responsibility of the help desk.	<p>The help desk policy should include the following:</p> <ul style="list-style-type: none"> ▪ how to submit support requests; ▪ how to prioritize/escalate; and ▪ who is responsible in the event of escalation.

Appendix D – Assessment of IT by COBIT Process

#	COBIT Process Objective ³	Risk Level ⁴	IT Maturity Level ⁵
1	PO1 – Define a Strategic IT Plan	Moderate	3
2	PO2 – Define the Information Architecture	Moderate	1
3	PO3 – Determine Technological Direction	Moderate	2
4	PO4 – Define the IT Processes, Organisation and Relationships	Low	2
5	PO5 – Manage the IT Investment	High	2
6	PO6 – Communicate Management Aims and Direction	Moderate	2
7	PO7 – Manage IT Human Resources	Moderate	2
8	PO8 – Manage Quality	Moderate	2
9	PO9 – Assess and Manage IT Risks	High	2
10	PO10 – Manage Projects	Moderate	3
11	AI1 – Identify Automated Solutions	Low	1
12	AI2 – Acquire and Maintain Application Software	Low	2
13	AI3 – Acquire and Maintain Technology Infrastructure	Moderate	2
14	AI4 – Enable Operation and Use	Low	1-2
15	AI5 – Procure IT Resources	Low	2
16	AI6 – Manage Changes	High	2
17	AI7 – Install and Accredite Solutions and Changes	High	2
18	DS1 – Define and Manage Service Levels	Moderate	3
19	DS2 – Manage Third-party Services	Moderate	2
20	DS3 – Manage Performance and Capacity	Low	1
21	DS4 – Ensure Continuous Service	Moderate	2-3
22	DS5 – Ensure Systems Security	High	1-2
23	DS6 – Identify and Allocate Costs	Moderate	3
24	DS7 – Educate and Train Users	Low	2
25	DS8 – Manage Service Desk and Incidents	Low	3
26	DS9 – Manage the Configuration	Low	1
27	DS10 – Manage Problems	Moderate	3
28	DS11 – Manage Data	High	2
29	DS12 – Manage the Physical Environment	Moderate	3
30	DS13 – Manage Operations	Moderate	2
31	ME1 – Monitor and Evaluate IT Performance	Low	1
32	ME2 – Monitor and Evaluate Internal Control	Moderate	2
33	ME3 – Ensure Compliance with External Requirements	High	1-2
34	ME4 – Provide IT Governance	Moderate	3

³ Overall evaluation is based on interviews with IT personnel as well as inspection of IT planning documentation, recent Internal Audit report observations, and various IT operational documentation during the course of this IT assessment.

⁴ A risk level of 'High' indicates that there is a significant level of inherent risk to IT security/confidentiality, integrity of data, or availability of systems. Medium' indicates that there is a moderate overall inherent risk, and 'Low' indicates a minimal inherent risk.

⁵ Based on the "Maturity Model for Internal Controls" documented in Appendix III of ISACA's COBIT 4.1. Refer to Appendix G of this report for Maturity Level descriptions. Processes that exhibited components of two different maturity levels were assigned both in the table above.

Appendix E – COBIT Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0: Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1: Initial/ <i>ad hoc</i>	There is some recognition of the need for internal control. The approach to risk and control requirements is <i>ad hoc</i> and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an <i>ad hoc</i> basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2: Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3: Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4: Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
	<p>reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.</p>	<p>of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.</p>
5: Optimised	<p>An enterprise-wide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.</p>	<p>Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.</p>