City of Santa Fe – Internal Audit

200 Lincoln Ave, Santa Fe, NM 87504-0909 (505) 955-5728, cell (505) 490-3372
Liza A. Kerr, Internal Auditor

Date: April 01, 2015

To: Brian Snyder, City Manager

From: Liza Kerr, Internal Auditor

RE: ITT Data Center Operations and IT General Controls Follow-Up Performance Audit

The Internal Audit Department performed a follow-up performance audit of the Information Technology and Telecommunications (ITT) Data Center Operations and Information Technology (IT) General Controls Performance Audit. The original audit included recommendations to ITT management.

The follow-up audit is substantially less in scope than the original audit. The objective and scope of the follow-up audit is to report on the status of corrective action taken by ITT to address the findings and recommendations from the original report.

The follow-up audit relies on ITT to provide the current status and supporting documentation for addressing the recommendations.

Internal Audit strongly supports a secure ITT environment, and urges the support of the City Manager, Mayor, and the Governing Body in this endeavor.

Liza Kerr, CIA, CISA, CPA, MBA
Internal Auditor

cc: Brian Snyder, City Manager
Javier Gonzales, Mayor
Kelley Brennan, City Attorney
Renee Martinez, ITT Director
Audit Committee
Accounting and Consulting Group

ITT Data Center Operations and IT General Controls Follow-Up Performance Audit

April 2015

OFFICE OF THE INTERNAL AUDITOR

CITY OF SANTA FE

Santa Fe: The City Different, The City Prepared

The Internal Audit Department and the role of Internal Auditor were created by City Ordinance No. 2012-32 and amended by City Ordinance No. 2013-34, Section 2-22 Santa Fe City Code (SFCC) 1987. A primary purpose of the Internal Auditor is to share a duty with the members of the governing body to insure that the actions of public officials, employees and contractors of the city are carried out in the most responsible manner possible and that city policies, budgets, goals and objectives are fully implemented. The Internal Auditor is also the City of Santa Fe's (the City's) liaison to the Audit Committee.

The Audit Committee was created by City Ordinance No. 2013-35, Section 6-5 SFCC 1987. This committee is an advisory committee and consists of five members of the community. Of the five members, one member shall be a certified public accountant, one member shall be a lawyer or have a law enforcement background and one member shall be a management consultant.

The Internal Auditor and the audit committee are structured in a manner to provide independent oversight of the City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

AUDIT COMMITTEE

Clark de Schweinitz, Esq., Chairman
Hazeldine Romero, Retired CIA, CPA, CGFM, Vice Chairman
Marc Tupler
Cheryl Pick Sommer

INTERNAL AUDITOR

Liza Kerr, CPA, CISA, CIA, MBA

Mission Statement

The mission of the City of Santa Fe Internal Audit Department is to provide independent, objective assurance and review services designed to promote transparency, accountability, efficiency, and effectiveness of City government for the citizens of the City of Santa Fe.

City of Santa Fe – Internal Audit
200 Lincoln Ave, Santa Fe, NM 87504-0909 (505) 955-5728, cell (505) 490-3372
Liza A. Kerr, Internal Auditor

AUDITORS' REPORT

The ITT Data Center Operations and IT General Controls Follow Up Performance Audit has been completed. The purpose of this follow-up audit was to ensure that the recommendations from the findings identified during the original 2013 audit have been implemented or otherwise resolved. These follow-up procedures are required by Government Auditing Standards Section 7.05 which requires the auditor to "facilitate follow-up to ensure that corrective action has been taken."

This follow-up performance audit is authorized pursuant to City of Santa Fe Ordinance 2013-34, §2-22.6. This follow-up audit was conducted in accordance with generally accepted governmental auditing standards, except for a peer review. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence provides a reasonable basis for our findings and conclusions based on our audit objectives.

Issues were still found in the areas of environmental controls including 1) lack of a redundant cooling system, 2) lack of water sensors and monitors, and 3) lack of fire suppression. Additional issues identified were 4) lack of a back-up generator, 5) no periodic review of data center access, 6) disaster recovery plan has not been tested, 7) IT security police has not been implemented, and 8) there is no annual testing of mirrored back-up of financial servers.

Internal Audit concludes that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited.

Internal Audit extends its appreciation to Renee Martinez, ITT Director and her staff who assisted and cooperated with us during the audit.

Liza Kerr, CIA, CISA, CPA, MBA
Internal Auditor

City of Santa Fe – Internal Audit
200 Lincoln Ave, Santa Fe, NM 87504-0909 (505) 955-5728, cell (505) 490-3372
Liza A. Kerr, Internal Auditor

EXECUTIVE SUMMARY

The purpose of this follow-up performance audit was to ensure that management has addressed and resolved the findings as cited in the original audit report.

Based on the results of the testwork, as summarized in the table below, ITT has made progress in improving the internal control environment. Although progress has been made, there is still opportunity for improvement regarding data center and information technology general controls.

The original audit report was issued in June of 2013, and can be found and downloaded from Internal Audit's website at http://www.santafenm.gov/internal_auditor. The link on the website is Data Center Operations Performance Audit.

Each original finding, and the associated sub-findings as applicable are designated with one of the following five (5) status categories:

Cleared	All aspects of the finding have been addressed by implementing the original corrective action, or an alternative corrective action.
In Process	Some aspects of the finding have been completely resolved. Other aspects of the finding have had action taken, but resolution is not complete.
Not Applicable (N/A)	The recommendation is no longer applicable due to changes in procedures or changes in technology.
Repeat	This finding has not been resolved and has not changed since the initial audit.
Repeat and Modified	No action has been initiated on any aspects of the finding, but due to changes in conditions or circumstances this finding has been modified.

The original audit report cited eight (8) grouped findings, or twenty seven (27) individual findings. Upon completion of the follow-up testwork, we have determined the status for each audit finding as outlined in the following table:

#	Description of Finding	# of Sub-Findings	Cleared	In Process	N/A	Repeat	Repeat and Modified
1	Lack of Environmental Controls in Data Centers	7	3	*3	1		
2	Deficiencies Regarding Redundant Power Supply in Data Centers	3	2	*1			
3	Lack of Adequate Physical Security in Data Centers	4	2		1		1
4	Lack of ITT entity Level Controls	3	2	1			
5	Lack of Formal Policies and Procedures	4	2	1			1
6	Daily Saves of Financial Data are Unsuccessful or Incomplete	1	1				
7	Lack of Formal Annual Testing of File Server Backups and Recovery Procedures	4	3			1	
8	File Server Backup is not occurring on non-financial data such as email, MS Word documents, Excel spreadsheets, and Share Drive documents	1	1				
	Summary	27	16	**6	2	**1	**2

* Findings 1 and 2 have 4 sub-findings that remain open. ITT has done everything that is within their direct control to resolve these issues, and are waiting for the funding for these initiatives. However, the findings will remain open until they are either funded or senior management makes a decision to assume the risk.

** There are 9 findings that remain open and will be carried forward.

SEE ATTACHMENT 1 for a mapping of the prior findings to the current report, and for a brief summary of the status of the findings and explanation of why/how a finding was cleared.

Table of Contents

INTRODUCTION AND BACKGROUND

The primary focus of the ITT division is to provide end-users with effective and cost-efficient tools through the use of advanced technology. ITT continually strives to offer state-of-the-art hardware and software applications, which ultimately provide the foundation for e-government and e-commerce services.

The City is a large and complex organization and the protection of its IT assets is of critical importance to its continued operations. It is imperative that these assets are protected, adequate back-up and disaster recovery controls are in place, and data backup and disaster recovery is tested well in advance of a disaster. The computer operations of the City are connected through a data network. The network connects all City locations where agencies have offices or information technology systems thus enabling business systems, telephones, and email to connect to data centers across town and the internet.

City offices with network connections include libraries, recreation centers, police and fire stations, and senior centers. Network connections are also utilized by systems not contained within offices, such as traffic control and video surveillance systems. Some agencies, such as libraries, also provide network connections to enable the public to access the Internet. Nearly all City agencies depend on the availability of the network to conduct their business and to provide services to the public, thus making the network a critical component of the City's information infrastructure. The ITT division manages this network which is housed in the data center.

As part of this follow-up audit a series of site visits occurred at the data centers that house City data. The purpose of these site visits was to get a first-hand view of the control environment at the data centers.

The data centers / server rooms at City Hall are outdated. The building itself is old and the cost of retrofitting the server rooms to industry standards needs to be weighed against the cost of having a third party host the servers. Renee Martinez, Director, ITT, is planning on making a recommendation to modernize the data center. This recommendation may include moving the data center to a more suitable facility. The findings noted will be cited, as this information may help provide senior management and the Governing Body with an objective overview of the current conditions.

SCOPE

Scope was limited to actions taken to address our recommendations or otherwise resolve the findings as cited in the ITT Data Center Operations and IT General Controls Performance Audit report dated June 2013.

OBJECTIVES

The objective of the follow-up performance audit is to ensure that the recommendations from the findings identified during the original 2013 audit have been implemented or otherwise resolved.

METHODOLOGY

To achieve the objective of the follow-up procedures we:

1) Conducted interviews with ITT management and staff;
2) Conducted a walkthrough of the ITT data centers;
3) Obtained and reviewed policies and procedures; and
4) Obtained and reviewed other evidence as necessary to validate the current status of the findings.

RESULTS

Elements of the unresolved findings are detailed below including:

1) Condition;
2) Criteria;
3) Cause;
4) Effect or Potential Effect;
5) Recommendation; and
6) Management's Implementation Plan and Date.

The original report grouped 27 findings into 8 large findings. This was done in situations where certain elements of the finding such as criteria, cause, and effect were identical. This report breaks the remaining open findings out, as this will allow Internal Audit and ITT to clear them individually, on a go-forward basis.

FINDING 1 – Lack of Redundant Cooling System
(Previously Finding 1.1, this finding is in the process of remediation).

Condition

During the initial audit while conducting the walkthrough, the temperature in the City Hall main data center was 81 degrees due to failure of the cooling system, and lack of a redundant cooling system.

During the walkthrough for the follow up audit it was noted that the temperature was 69 degrees, however, there is still no redundant cooling system.

Criteria

Appropriate internal controls as related to the data center environment should exist to ensure the security and reliability of equipment in the data centers. These internal controls include temperature controls.

Cause

Internal controls pertaining to physical environment in the City's data centers are not always effective. These deficiencies in the internal control environment can affect operations of the City. Specifically, the City lacks a redundant cooling unit for the City Hall data center.

Effect or Potential Effect

Heat weakens electronic components like power supplies, motherboards, and memory chips, so even if they don't fail immediately, they become more susceptible to failure over time. This can result in node crashes, and erratic and weakened electronic parts that are more vulnerable to failure on a go forward basis. The true repercussions of overheating may not become apparent for several months. This is a critical issue since the financial, email and network servers are all located in this room. The loss of any of these servers could result in critical downtime for City operations, the loss of financial and other data, and may also impact the City's credibility and public image. The cost of replacing these servers, the downtime that might result due to data loss, and the restoration of public image far exceeds the cost of a redundant cooling system and preventive maintenance.

Recommendation

Continue to pursue a funding source for a redundant cooling system until this finding is resolved or senior management makes a decision to assume the risk.

Management's Implementation Plan and Date

Per ITT management, a budget increase request was made for a standby/redundant air conditioning unit. This budget increase was denied. There is a budget expansion request in at this time, for this item. In addition, ITT management stated that there might be some money available using Capital Improvement Project (CIP) bond funds. ITT will continue to request the money, but are limited to the budgetary approval process. Another option under consideration is

to move the City data center to more suitable location with adequate cooling, fire suppression and power systems.

The ITT Director is planning on making a recommendation to modernize the data center. This recommendation may include moving the data center to a more suitable facility making the purchase of a redundant cooling system unnecessary.

This finding is expected to be resolved during FYE 2015.

FINDING 2 - Lack of Water Sensors and Monitors
(Previously Finding 1.2, this finding is in the process of remediation).

Condition

During the walkthroughs of the Santa Fe Police Department (SFPD) data center and the Communications Room at City Hall it was noted that there are no water sensors under the raised floor, or other monitoring system to alert ITT personnel of the presence of water. This is especially problematic for the Communications Room as there is a history of flooding due to burst pipes in the building.

Criteria

Appropriate environmental controls should exist to ensure the security and reliability of equipment in data centers. Such controls include water sensors and monitoring systems.

Cause

Internal controls pertaining to water detection and monitoring are non-existent at SFPD and in the Communications Room.

Effect or Potential Effect

Flooding can cause equipment failure or loss of data in the data centers.

Recommendation

Continue to pursue a funding source for water sensors and monitoring systems until this finding is resolved or senior management makes a decision to assume the risk.

Management's Implementation Plan and Date

Per ITT management, a budget increase request was made for a Moisture Detection and Alarm System. This budget increase was denied. There is a budget expansion request in at this time, for this item. In addition, there might be some money available using CIP funds. ITT will continue to request the money, but are limited to the budgetary approval process.

This finding is expected to be resolved during FYE 2015.

FINDING 3 – Lack of Fire Suppression
(Previously Finding 1.3, this finding is in the process of remediation).

Condition

None of the three data centers (SFPD, City Hall, and Communications Room) has fire suppression, although, hand held chemical extinguishers are available.

Criteria

Appropriate environmental controls should exist to ensure the security and reliability of equipment in data centers. Such controls include fire suppression systems. It is best to prevent fires altogether and to take whatever precautions can be taken up front to ensure that this issue never has to be dealt with. Fire prevention includes protecting wiring, removing clutter, and other safeguards that are typically low cost, but deliver high returns.

Cause

Internal controls pertaining to adequate fire suppression in the data centers are not adequate.

Effect or Potential Effect

Fire in a data center is self-explanatory. The damage that is caused is typically irreparable and extensive. The damage can be from the fire itself, smoke or even from water based products used to contain or put out the fire. The axiom 'an ounce of prevention is worth a pound of cure' certainly applies here.

Recommendation

Continue to pursue a funding source for fire suppression until this finding is resolved or senior management makes a decision to assume the risk.

Management's Implementation Plan and Date

Per ITT management, a budget increase request was made for a Fire Suppression System. This budget increase was denied. There is a budget expansion request in at this time, for this item. In addition, there might be some money available using CIP funds. ITT will continue to request the money, but are limited to the budgetary approval process. The ITT Department Director has approved using existing operating budget to purchase a moisture detection and alarm device for all three sites using FY14-15 monies.

This finding is expected to be resolved during FYE 2015.

FINDING 4 – Lack of a Back-Up Generator
(Previously Finding 2.1, this finding is in the process of remediation).

Condition
There is no backup generator at City Hall. This affects both the City Hall main data center and the Communications Room.

Criteria
Appropriate environmental controls should exist to ensure the security and reliability of equipment in data centers. Such controls include a redundant power supply including back-up generators where key data is processed.

Internal controls regarding redundant power are necessary to prevent single points of failure. This redundancy helps to assure continued operations in the case of a power failure.

Cause
Internal controls pertaining to redundant power in the City's data centers are not adequate.

Effect or Potential Effect
Not having a redundant power source in the data centers can result in costly down time in the event of a power failure.

Recommendation
Continue to pursue a funding source for a back-up generator.

Management's Implementation Plan and Date
Estimates for a back-up generator for City Hall and the Communications Room have been received. ITT management requested a budget increase for a back-up generator for the two datacenters at City Hall. This budget increase was denied. There is a budget expansion request in at this time, for this item. In addition, there might be some money available using CIP funds. If so, this item is at the top of the list. ITT will continue to request the money, but are limited to the budgetary approval process.

The ITT Director is planning on making a recommendation to modernize the data center. This most likely will include the suggestion of relocating to a more suitable facility. This recommendation may include moving the data center, making a backup generator unnecessary.

This finding is expected to be resolved during FYE 2015.

FINDING 5 – No Periodic Review of Data Center Access
(Previously Finding 3.2, this finding is repeat and modified).

Condition

There was no evidence of a periodic review of users with access to the City Hall main data center. During the follow up audit we requested a list of all users with access to the City Hall data center. A review of this list indicated one employee who no longer worked in ITT, one employee with a card issued in her maiden name and another issued in her married name, and four other employees with multiple keys.

Criteria

A formal annual review needs to be done of people that have access to the data center. Employees and vendors that no longer need access should be removed, and multiple keys need to be deleted. Evidence of this review needs to be retained for audit purposes.

Cause

Internal controls relating to data center physical security are not adequate.

Effect or Potential Effect

Not terminating access for employees or vendors that no longer need it or deleting swipe cards when additional ones are made due to loss or other reasons, may result in unauthorized access and or loss or damage to assets or data.

Recommendation

A formal annual review needs to be done of people that have access to the data center. Employees and vendors that no longer need access should be removed, and multiple keys need to be deleted. Evidence of this review needs to be retained for audit purposes.

Management's Implementation Plan and Date

A review was completed in November 2014 and employees no longer needing access were removed from the electronic system. A formal annual review will be conducted in November of each year moving forward.

Internal Audit's Response

The review of data center access referenced above was actually done by Internal Audit on November 13, 2014. Users were removed at the request of Internal Audit. This finding remains open until Internal Audit receives evidence of a 1) periodic review initiated and done by ITT, and 2) formal written policy or procedure indicating an annual review, or review when an employee leaves and no longer needs access.

FINDING 6 – Lack of Security Assessment of Outside Service Providers
(Previously Finding 4.3, this finding is in process).

Condition

ITT is not assessing the security environment and internal controls of outside service providers who provide or house significant financial data for the City.

ITT management has begun to compile a list of outside service providers that house financial data for the City. At the time of the audit the list did not include collaboration with Finance, Parking, Water Utilities or other departments that use a third party provider to house financial data. Nor is there any indication of whether or not the vendors on the list have adequate IT security controls to protect the City's data.

Standard procedures include obtaining a Service Organization Control (SOC) report commonly referred to as a Standards for Attestation Engagements (SSAE) 16, SOC 1 or SOC 2, if available. If not available, an IT security audit should be done to ensure that the IT controls protecting our data are properly designed and are effective.

Criteria

Outside service providers that are providing a material financial service to the City need to have adequate security and internal controls in place so that City data or services to the City are not compromised.

Cause

Internal controls pertaining to outside service providers are not clearly identified, nor has a determination been made as to their effectiveness.

Effect or Potential Effect

Not assessing the security and internal controls of outside service providers may result in unacceptable downtime, security breaches, and loss of data, and damage to the City's reputation.

Recommendation

ITT management needs to assume ownership and accountability for this process. It is recommended that they collaborate with finance and other key departments such as parking to determine which vendors house financial data for the City. ITT then needs to determine that each vendor on the list has adequate internal controls regarding IT security to ensure protection of the City's data.

Industry standards allow the City to obtain a report from the vendor's auditor so that work does not have to be duplicated. This report is a referred to as an SSAE 16, SOC 1 or SOC 2. These reports should be obtained where possible so that the City does not have to incur additional audit fees, and if not, other measures including doing a vendor audit should be taken.

Management's Implementation Plan and Date

ITT management is in the process of compiling a list of vendors that house financial data. ITT management also feels strongly that the Departments that are sponsors of information systems that house financial data should share responsibility with ITT to own and be accountable for this process. Also, the ITT Department's annual security assessment, conducted by a third party, was completed in March with an emphasis on City systems that must be PCI compliant as they process credit card transaction. Remediation of PCI vulnerabilities has started and are planned to be completed by June 2015.

Internal Audit's Response

This finding remains open until someone in senior management assumes leadership and initiates a process or procedure of obtaining SOC 1's or SOC 2's, if available, or otherwise assessing the vendor's internal control structure regarding IT security. Implementation dates are required to clear the finding.

FINDING 7 – Disaster Recovery Plan Not Tested
(Previously Finding 5.2, this finding is repeat and modified)

Condition

ITT now has a formal, written Disaster Recovery Plan; however, the plan has not been tested.

Criteria

Drafting a formal, written disaster recovery plan is the first step in a process. The next step is to ensure the plan will work by testing it.

Cause

The formal disaster recovery plan has just been recently implemented.

Effect or Potential Effect

The plan may not work or may need to be fine-tuned. If the plan were to fail in the event of a disaster it could result in:

1) Destruction of data,
2) Incomplete, inaccurate and untimely recovery of data, and
3) Cessation of business operations.

Recommendation

Test the disaster recovery plan. Implementation date is required.

Management's Implementation Plan and Date

A test of the disaster recovery plan for all systems running on the IBM iSeries hardware platform which include the financial accounting and payroll system and business licensing system is planned for May 2015. A disaster recovery process is in place for employee and department documents stored on the City storage area network. File servers housed in the Police Department server room are updated in real-time to mirror changes on the primary file servers housed at the City Hall Data Center.

Internal Audit's Response

This finding remains open until plan has actually been tested, and evidence of testing and results are provided to Internal Audit.

FINDING 8 – IT Security Policy Not Implemented
(Previously Finding 5.3, this finding is repeat and modified)

Condition

The IT Security Policy drafted by Cannes, a contractor engaged to perform a Security Assessment and to draft the Security Policy has not been implemented.

The IT Security Policy drafted by Cannes references a designated IT Security Officer. ITT does not have a designated IT Security Officer so they have not implemented the policy.

Criteria

Formal policies and procedures need to exist, and need to be implemented, regarding IT Security.

Cause

An internal control environment for IT security that is clearly defined in policies and procedures exists, but has not been implemented. This is creating a weak internal control environment which can affect operations of the City. ITT lacks sufficient resources to implement the security policy.

Effect or Potential Effect

Not having clearly defined security policies and procedures may result in:

1) Information systems that are not available and useable when required (availability);
2) Data and information that are disclosed to those that do not have a right to know (confidentiality); and
3) Data and information that are not protected against unauthorized modifications (integrity).

Recommendation

Implement the IT Security Policy.

Management's Implementation Plan and Date

The City has a policy for Technology Use that includes information security requirements for employees. The ITT Director has included a new position for an Information Security Officer in the Department budget request for FY15-16. This positon will responsible for establishing and managing security policy and procedures based on industry best practices.

Internal Audit's Response

In the Technology Use Policy mentioned above, Section 5.0 addresses IT Security. It is two sentences long. The first sentence addresses password length and complexity, the second addresses privacy expectations (in most cases, there are none as all records are open). This finding remains open until a comprehensive IT Security Policy has been implemented.

FINDING 9 – No Formal Annual Testing of Mirrored Back-Up of Financial Servers
(Previously Finding 7.1, this finding is repeat and modified)

Condition

Formal annual testing of the file servers doing mirrored backup of the I-Series financial data is not being done at the Regional Emergency Command Center (RECC) and or evidence of back-up procedures are not retained.

Criteria

A formal annual test of file server recovery / procedures needs to occur to ensure data integrity and disaster recovery capabilities.

Cause

Internal controls pertaining to annual testing of file server recovery / procedures are not effective. These deficiencies in the internal control environment can affect operations of the City.

Effect or Potential Effect

Not performing an annual test on file server recovery / procedures to ensure data integrity and disaster recovery capabilities may result in a failed recovery in the event of a disaster. This may impact the City's ability to continue with business operations. The City may not be able to recover data in the event of a disaster.

Recommendation

Develop a plan for annual testing of data recovery of file servers at RECC that are mirroring the City's financial data.

Management's Implementation Plan and Date

IT Management will enlist the assistance of Visions Solutions to engage in a contract to conduct three virtual role swaps and three live role swaps of the logical partitions for the City's IBM System I (iSeries or AS400). The deliverables for this contract will include documentation and training of IT staff. IT will engage in a professional services agreement this fiscal year and the work is planned for May 2015. IT's goal will be to conduct role swaps on annual basis with test results maintained for not less than 36 months.

APPENDIX

(SEE ATTACHMENT 1 – FINDINGS SUMMARY)

SUMMARY OF FINDINGS - From Original Audit Report

	WP FINDING 1 Series B	New Finding #	Current Status	
1.1	The temperature in the City Hall data center / server room was 81 degrees on the day of the walkthrough. See B.1.c on WP lead sheet	1	In Process	ITT is in the process of remediating this finding. They have requested funding to do this. The budget increase was not approved, but the money should be available through CIP funds sometime during FYE 2015. Although data center was cool on the day of the walkthrough management is looking for a redundant cooling system for the city hall data center.
1.2	The SFPD data center, and the secondary data center at City Hall, (communications room) do not have water sensors or a monitoring system to alert ITT personnel of the presence of water. This is especially problematic for the communications room as there is a history of flooding due to burst pipes in the building.	2	In Process	ITT is in the process of remediating this finding. They have requested funding to do this. The budget increase was not approved, but the money should be available through CIP funds sometime during FYE 2015.
1.3	None of the three data centers (SFPD, City Hall, and communications room) has fire suppression, although, hand held chemical extinguishers are available.	3	In Process	ITT is in the process of remediating this finding. They have requested funding to do this. The budget increase was not approved, but the money should be available through CIP funds sometime during FYE 2015.
1.4	Wiring in the City Hall data center is not protected from fraying on edges of raceway / rack and poses a fire risk		Cleared	Verified through visual inspection.
1.5	There was significant clutter comprised of combustible material in the communications room, which is a fire code violation		Cleared	Verified through visual inspection.
1.6	The three phase main feed in the communications room does not have a protective cover and poses a fire risk		N/A	Per fire marshall - cannot put a cover on this panel.
1.7	1.1.a. Cooling unit in the City Hall data center is not receiving routine maintenance by a technician certified on these types of units.		Cleared	Verified by inspecting maintenance records. ***Note - this finding is really 1.1 a, but moved here so that numbering of 'sub findings' would match bullet points from original audit report.***
	WP FINDING 2 **Series C**			
2.1	Lack of a back-up generator for 2/3 data centers	4	In process	ITT is in the process of remediating this finding. They have requested funding to do this. The budget increase was not approved, but the money may be available through CIP funds sometime during FYE 2015.

2.2	Lack of routine maintenance on back-up generator at SFPD		Cleared	Verified by inspecting maintenance records.
2.3	Lack of routine maintenance on the Uninterruptable Power Supply (UPS) at 3/3 data centers		Cleared	Verified by inspecting maintenance records.

WP FINDING 3 - Lack of Physical Security in the Data Centers

Series D

3.1	Door to the ITT offices at City Hall was left unlocked over the weekend starting Friday, 03/08/2013 and ending Monday morning 03/11/2013. This was captured on video tape. During the walkthrough on 03/08/2013, internal audit observed the door to the Communications Room at City Hall had not been locked.		Cleared	Verified by personal inspection.
3.2	Physical access to the server rooms is not always restricted to authorized personnel, and is not reviewed on a periodic basis.	5	Repeat and Modified	A list of all users with swipe card entry was obtained from ITT. A review of the list indicated several users that need to have access disabled. ***There is no indication of a periodic review of user access.***
3.3	At the time of this audit vendors were not required to fill out user authorization forms to gain access to the data center.		N/A	A list of all users with access to the data center was obtained. There are only 2 vendors with access to the data center. ***Given this, pass on this finding.***
3.4	Entry to the data center at City Hall is through the use of a key pad. Anyone with the code may enter. Currently, the ability to track who has gone in is not available, just the times that they enter.		Cleared	Per verification with EJ Duran at the City Hall Main Data Center, the keypad sequence was changed recently when a City Employee that had access to the data center left and no longer needed it. It should be noted that swipe card access is also being used at the Data Center. See 3.2 above.

WP FINDING 4 - Lack of ITT General Controls

Series E

4.1	Lack of a steering committee.		Cleared	A new committee titled IT Governance Committee was formed and had a meeting on February 10, 2015. The Charter was approved at that meeting. The next meeting is scheduled for April 14, 2015.
4.2	Lack of a formal, annual risk assessment.		Cleared	Presidio and Cannes assessments are both excellent risk assessments.

4.3	Not assessing the security environment and internal controls of outside service providers who provide significant financial services to the City.	6	In Process	ITT Management has a list of vendors that they do business directly with - who are storing data for ITT. This needs to expanded to vendors that Finance or other City Departments are using to store financial data. ITT needs to determine that the security controls over our financial data are adequate. One way of doing this is by obtaining an SSAE16.
WP Series F	**FINDING 5 - Lack of Formal Policies and Procedures**			
5.1	1) Risk assessment - There is no formal, annual risk assessment process, and there are no formal policies and procedures regarding the risk assessment process.		Cleared	Formal Risk assessment policy completed by ITT.
	Back-up, Data Retention and Disaster Recovery			
5.2	There is no disaster recovery plan.	7	Repeat and Modified	**Phase 2 - the plan needs to be tested.**
5.2a	There is a schedule of when backups are to be performed, and an understanding of how long they are to be retained, but this is not documented in a formal policy. Also, retention of backups does not take into account City or State data retention requirements.		Cleared	ITT uses the state and city data retention guidelines.
5.3	Security - ITT does not have a comprehensive formal information security policy or procedures manual. Lack of a comprehensive ITT security policy has been cited as a finding by different auditors for several years. This is a repeat finding, and stating that a draft exists is no longer an acceptable response.	8	In Process	A security policy was obtained from Cannes, but ITT has stated that they are unable to implement the policy due to them not having a designated Security Officer. **This finding is *in process*** and will remain open until the policy is implemented. The ITT ploicy needs to be implemented in whole or in part.
WP Series G	**FINDING 6 - Daily Saves of Financial Data Are unsuccessful or Incomplete**			
6.1	An error message stating the daily saves on the financial servers "are unsuccessful or incomplete" is occurring on all 4 LPARS.		Cleared	**This finding has been *cleared.*** Per discussion with Zeke Perea, Network Specialist, he was able to correct this issue for 2 of the 4 LPAR's. For the remaining 2 LPAR's he has determined that the data that is not being saved is non-essential data. In order to ensure that the message does not in fact indicate an issue he verifies on a daily basis the libraries that are saved and thereby ensures that all critical data has been saved.
WP Series H	**FINDING 7 - Lack of formal annual testing of file server back-ups and recovery procedures**			

7.1	A formal annual testing of the file servers doing mirrored backup of the I-Series financial data is not being done. ITT is in the process of negotiating a contract with Vision Solutions - iTera to provide this service, but it is not expected to occur until after July 1, 2013. The contract would include three virtual roll swaps and three actual backups over the course of a year.	9	Repeat	This did not occur - this finding is not resolved.
7.2	A formal annual testing of the file servers doing mirrored backup of the non-financial data is not being done.		Cleared	Per Renee Martinez, ITT Director, **this finding is *cleared***. A disaster recovery process is in place for employee and department documents stored on the City storage area network. File servers housed in the Police Department server room are updated in real-time to mirror changes on the primary file servers housed at the City Hall Data Center.
7.3	Internal Audit was unable to verify a full restore on either the weekly or the annual system saves due to capacity issues in the test environment. ITT is planning on building a test LPAR in July 2013 that will have sufficient capacity to allow them to do this.		Cleared	Per Caryn Fiorina, they were able to do an upgrade on the test LPAR when they updated to 7.1 OS for iseries and were able to do full test for all applications that run on 7.1. The big exception here is payroll which runs on Enterprise 1 version 5.4. In order to test payroll they has to take the test LPAR back to the version of payroll which is 5.4. The LPAR is still at 5.4, but can be upgraded to 7.1 if needed.
7.4	City and State data retention requirements for electronic data may not be retained for the appropriate time periods.		Cleared	**This finding has been *cleared***. Per ITT they use the City and State Data Retention Ordinances.

WP FINDING 8 - File Server Backup

Series I

8.1	File server backup is not occurring on non-financial data such as email, MS Word documents, Excel spreadsheets, and Share Drive documents.		Cleared	Per Bill Smith, IT, the City was able to make this operational using DFS (distributed file system) in 2013.

Conclusion	While some improvements have been seen in the data center environment, and regarding ITT internal controls, there is still room for improvement. These deficiencies in the internal control environment can affect operations of the City. Based on the review, ITT has taken action and requested budgetary increases to cover the necessary expense of implementing these basic environmental controls. Budget increases were not approved during the last budget session. However ITT has informed internal audit that they will have monies available through CIP funding sometime during FYE 2015. Several findings remain open until a decision is made to make the required changes or not. Other findings are being worked on, but have not been fully resolved.