

ITT Data Center Operations and IT General Controls Performance Audit

JUNE 2013

INTERNAL
AUDIT
DEPARTMENT

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 on October 30, 2012. 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 liaison to the Audit Committee.

The Audit Committee was created by Resolution 2010-83 on October 13, 2010. This committee is an advisory committee and consists of 5 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

Maurice A. Lierz, Retired CPA, Chair

Randy Randall

Hazeldine Romero-Gonzales, Retired CIA, CPA, CGFM

Clark de Schweinitz, Esq., JD

Marc Tuppler

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
Liza A. Kerr, Internal Auditor

(505) 955-5728, cell (505) 490-3372

Date: August 15, 2013
To: Brian Snyder, City Manager
From: Liza Kerr, Internal Auditor
RE: Data Center Audit

Attached is the Internal Audit Department's report of the audit of the City of Santa Fe's data centers. The purpose of this audit was to determine that:

- 1) Adequate levels of physical security and fire protection, flood protection, and power protection are provided for computer equipment and data files.
- 2) Sufficient controls exist to protect data files and programs from accidental loss.
- 3) Protective measures are taken to ensure that operations of the location can continue without serious interruption in the event of a disaster that results in loss of the center.

Special thanks are given to all of the Information Technology and Telecommunication (ITT) staff for their cooperation during the course of the audit.

The audit presents findings in the area of environmental controls including temperature control, flood detection and monitoring, fire suppression, fire prevention, physical security of the data center, power supply, data backup and disaster recovery, as well as general matters such as lack of formal policies and procedures.

Vulnerabilities that may have existed for years can no longer be ignored as threats to information systems have become more prevalent. The ramifications for information security breaches, data loss, and the inability to continue operations due to systems failures are well within the public's awareness. Failures in these areas are preventable. The cost of regaining public confidence after a preventable disaster far outweighs the cost of prevention. Certainly the idiom "an ounce of prevention is worth a pound of cure" applies here.

A much needed analysis comparing the cost/benefit of retrofitting the current data centers to comply with industry standards versus moving to a hosted site is currently in process with an independent contractor.

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

If you have questions, please contact Liza Kerr, Internal Auditor, at (505) 955-5728.

cc: Thomas Williams, Division Director, ITT
Marcos Tapia, City Finance Director
David Coss, Mayor
Geno Zamora, City Attorney
Members of the Audit Committee
Members of the Governing Body
Atkinson and Company, External Auditor



City of Santa Fe – Internal Audit

200 Lincoln Ave, Santa Fe, NM 87504-0909
Liza A. Kerr, Internal Auditor

(505) 955-5728, cell (505) 490-3372

AUDITORS REPORT

The audit of the data centers has been completed. The purpose of this audit was to determine that adequate controls exist and are effective within the City's data centers to ensure that:

- 1) Adequate levels of physical security, fire protection, flood protection, and power protection are provided for computer equipment and data files.
- 2) Sufficient controls exist to protect data files and programs from accidental loss.
- 3) Protective measures are taken to ensure that operations of the location can continue without serious interruption in the event of a disaster that results in loss of the center.

This performance audit is authorized pursuant to City of Santa Fe Ordinance 2012-32, §2-22.6. This performance 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.

Significant issues were found in the areas of environmental controls including temperature control, fire detection, fire suppression, fire prevention; as well as physical security of the data center, redundant power supply, data backup and disaster recovery, and general matters such as lack of formal policies and procedures.

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 Thomas Williams, ITT Division Director and his staff who assisted and cooperated with us during the audit.

Specific information related to indications of potential fraud, waste and abuse are included in a separate report to the City Manager, and the City Finance Director to determine proper action. This separate report is not considered confidential and will also be provided to the Audit Committee, the Governing Body, and the Independent Public Accountant in accordance with governmental auditing standards and City of Santa Fe Ordinance 2012-32 § 6, 2-22.5 A.

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

Table of Contents

EXECUTIVE SUMMARY 1

INTRODUCTION AND BACKGROUND 2

SCOPE..... 2

OBJECTIVES 3

METHODOLOGY 3

RESULTS 4

 Site Visits..... 4

 Site Visit of City Hall Data Center..... 4

 Site Visit of City Hall Secondary Data Center (Communications Room) 5

 Site Visit of Santa Fe Police Department Data Center 5

 Hitachi Storage Area Network (SAN) 5

 Data Backup and Disaster Recovery 6

 Backup of I-Series Financial Data..... 6

 Tape Backups of Financial Data 6

 File Server Mirrored Backup 7

 Tape Backup of Email, Word, Excel, and Share Drive Documents..... 8

 Testing of Internal Controls as Identified By External Auditors..... 8

FINDING 1..... 12

 Condition..... 12

 Criteria 12

 Cause..... 12

 Effect 12

 Recommendation..... 13

 Management’s Response and Implementation Date 13

 Evaluation of Management’s Response..... 16

FINDING 2..... 16

 Condition..... 16

 Criteria 16

 Cause..... 17

 Effect 17

 Recommendation..... 17

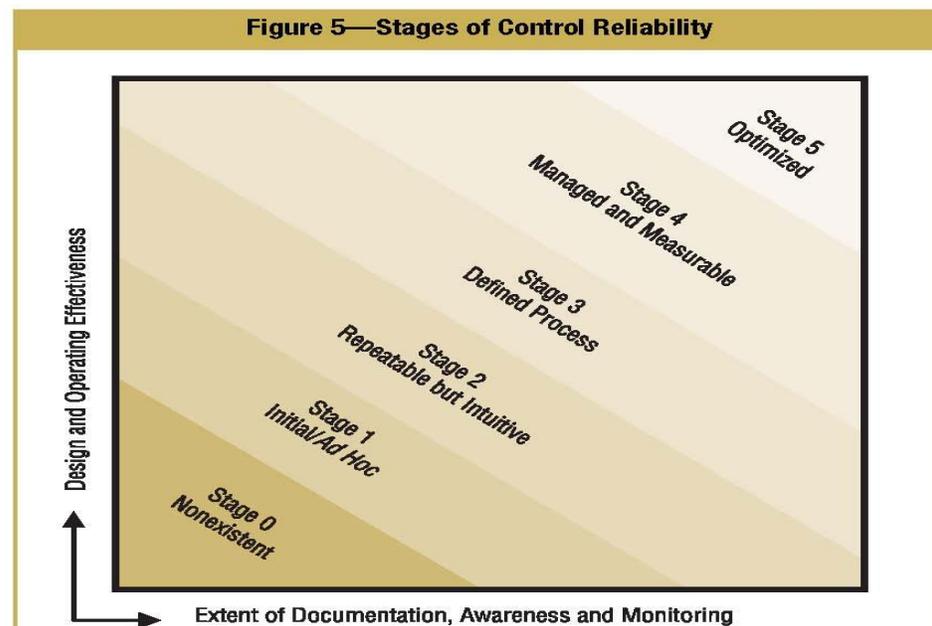
Management’s Response and Implementation Date	18
Evaluation of Management’s Response.....	18
FINDING 3.....	19
Condition.....	19
Criteria	19
Cause.....	19
Effect	19
Recommendation.....	20
Management’s Response and Implementation Date	20
Evaluation of Management’s Response.....	21
FINDING 4.....	21
Condition.....	21
Criteria	21
Cause.....	21
Effect	22
Recommendation.....	22
Management’s Response and Implementation Date	22
Evaluation of Management’s Response.....	24
FINDING 5.....	24
Condition.....	24
Criteria	25
Cause.....	25
Effect	25
Recommendation.....	26
Management’s Response and Implementation Date	26
Evaluation of Management’s Response.....	26
FINDING 6.....	27
Condition.....	27
Criteria	27
Cause.....	27
Effect	27
Recommendation.....	27

Management’s Response and Implementation Date	27
Evaluation of Management’s Response.....	28
FINDING 7.....	28
Condition.....	28
Criteria	28
Cause.....	28
Effect	28
Recommendation.....	29
Management’s Response and Implementation Date	29
Evaluation of Management’s Response.....	29
FINDING 8.....	29
Condition.....	29
Criteria	29
Cause.....	29
Effect	30
Recommendation.....	30
Management’s Response and Implementation Date	30
Evaluation of Management’s Response.....	30
APPENDIX.....	31
Pictures	31
Data Back-up and Recovery	35

EXECUTIVE SUMMARY

The key findings in the report are related to insufficient internal controls. The internal control environment in any information technology (IT) environment is enhanced when entity level controls are formalized and a good foundation of policies and procedures exists. While the Information Technology and Telecommunications (ITT) division has considerable inherent knowledge between all of the staff, there is an opportunity to enrich the division by creating formal policies and procedures. This would enable the division to train new employees and would also help to ensure that the complex processes and procedures that they have to deal with on a daily, weekly, monthly, and annual basis are done consistently and efficiently.

The following chart illustrates a capability maturity model for an IT organization. This chart illustrates various stages of documentation starting with “Stage 0 Nonexistent”, and “Stage 5 Optimized”. The City’s ITT division would best be characterized as falling somewhere between Stages 1 and 3. While some policies and procedures are well-defined, others are ad hoc and informal. Even well-defined procedures are not formalized. As the department matures, and starts formalizing policies and procedures they move along the continuum to the next stage of control reliability. The goal is not to move from Stage 1 to Stage 5, but rather to slowly move through each of the stages to an optimized state.



¹ IT Control Objectives for Sarbanes Oxley, The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, September 2006, IT Governance Institute, pg. 38.

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 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. Pictures were taken to supplement the report and to give the reader a visual basis for understanding the information presented.

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. Thomas Williams, Director, ITT, is currently working with a consultant to evaluate these costs. 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

The scope of the audit included:

- 1) Performing an internal control assessment of the environment and security of all City data centers including City Hall and the Santa Fe Police Department.
- 2) Testing of internal controls as related to:
 - a. Entity level controls,
 - b. Data back-up and disaster recovery, and
 - c. Policies and procedures impacting data back-up and recovery, and security.

OBJECTIVES

The objectives of the audit were to:

- 1) Gain an understanding of the security and internal control environment within the City's data centers.
- 2) Determine if the internal controls identified by the external auditors and asserted to by ITT management exist, are designed effectively, and are operating as designed.

Our audit objectives were designed to ensure that:

- 1) Adequate levels of physical security, fire protection, flood protection, and power protection are provided for computer equipment and data files.
- 2) Sufficient controls exist to protect data files and programs from accidental loss.
- 3) Protective measures are taken to ensure that operations of the location can continue without serious interruption in the event of a disaster that results in loss of the center.

Accordingly, we used procedures including examination of records, voluntary interviews with appropriate personnel, vendors, and others, and other procedures as deemed necessary to accomplish our objectives.

METHODOLOGY

The following methodology was used:

- 1) Phase 1 – Walkthrough & Information Gathering
 - a. During this phase a physical walkthrough was done at each site. Information was gathered and documented regarding current conditions,
 - b. Documentation was obtained regarding policies and procedures, alerts used, follow up on alerts, back-up and disaster recovery procedures.
- 2) Phase 2 - Field Work
 - a. During this phase of the audit, site visits occurred to physically see where back-up is being stored or mirrored,
 - b. Testing of effectiveness of backups was also done.
- 3) Phase 3 – Wrap up and Report
 - a. During this phase of the audit, all of the gathered information was analyzed for presentation in a report to management. A detailed list of findings is included.

RESULTS

Site Visits

The purpose of the site visits was to evaluate the internal control environment for physical security, fire protection, flood protection, and redundant power for computer equipment and data files.

Site Visit of City Hall Data Center

The walkthrough of the main data center/server room at City Hall was done over the course of several days starting on 03/07/2013 and ending on 03/15/2013. Numerous internal control deficiencies were noted in regards to the physical environment. During the initial walkthrough on 03/07/2013 the temperature in the data center was 81 degrees. The temperature in a data center should be approximately 72 degrees. Attempts were being made to circulate the air to bring down the temperature. A call was put in to building maintenance to have them come out and help with this issue. In a second site visit on 03/08/13 building maintenance had still not responded to the service call, and while temperatures were slightly cooler, they had not reached 72 degrees. The decrease in temperature was attributed to the ITT staff changing the air filters in the cooling system. Since the financial, email and network servers are all located in this room this is a critical issue. The loss of any of these servers could result in critical downtime for City operations, and the loss of financial and other data. The cost of replacing these servers and the downtime that might result due to data loss far exceeds the cost of preventive maintenance, and a redundant cooling system for the server room.

The following internal control deficiencies were noted during the City Hall data center walkthrough:

- 1) The temperature in the main server room was 81 degrees, **(See Finding 1)**,
 - a. The Carrier cooling system in the main data center at City Hall is not receiving routine maintenance,
 - b. The response time of building maintenance in regards to cooling issues in the server room is not adequate.
- 2) There is no fire suppression in the data center **(See Finding 1)**.
 - a. A hand held extinguisher is available.
- 3) The wiring in the City Hall data center is draped directly over the racks edge with combustible material placed beneath to protect the lines from fraying **(See Finding 1)**, **(See Appendix - Pictures #5)**.
- 4) On Monday 03/11/2013 it was found that the door to the ITT offices, which lead to the data center, was left open over the weekend **(See Finding 3)**. This was documented on a video tape. The tape clearly showed that the last person leaving the Friday before had not properly closed the door.
- 5) The Uninterrupted Power Supply (UPS) is not receiving routine preventive maintenance **(See Finding 2)**.
- 6) There is no back-up generator to provide redundant power **(See Finding 2)**.

Site Visit of City Hall Secondary Data Center (Communications Room)

The following internal control deficiencies were noted:

- 1) On 3/8/13 the door to the basement data center (Communications Room) was found unlocked **(See Finding 3), (See Appendix - Pictures #3)**.
- 2) There was significant clutter comprised of combustible material in the Communications Room, some of which was piled in front of an electrical panel **(See Finding 1), (See Appendix - Pictures #2)**.
- 3) The three phase main feed in the Communications Room does not have a protective cover **(See Finding 1), (See Appendix - Pictures #4)**.
- 4) There is no fire suppression in the Communications Room. Per the City of Santa Fe Fire Marshall if fire caulking were used to plug up the holes in the room it could be rated as a two hour fire room. In other words a fire could be contained for two hours before spreading. This would give fire crews plenty of time to respond in the event of a fire **(See Finding 1)**.
- 5) There are no water sensors under the raised floors **(See Finding 1)**.
- 6) Uninterrupted Power Supply (UPS) **(See Finding 2)**.
 - a. The UPS system for the 911 data base has never had routine maintenance.

Site Visit of Santa Fe Police Department Data Center

The following environmental control deficiencies were noted:

- 1) There are no water sensors under the raised floors **(See Finding 1)**.
- 2) There is no fire suppression in the data center **(See Finding 1)**.
- 3) The UPS is not receiving routine preventive maintenance **(See Finding 2)**.
- 4) The generator is not receiving routine preventive maintenance **(See Finding 2)**.
 - a. In an attempt to save money, management discontinued the contract for routine maintenance and has requested these services be provided by Fleet Management.
 - b. On 06/21/2013, the Rich Bemis, Facilities and Evidence Manager, SFPD, stated that Fleet Management came out to service the generator and damaged it. Mr. Bemis commented that a radiator hose had cracked and needed to be replaced. The water was drained out of the generator so that they could replace the hose, but the heat pump was not turned off and ended up burning up. This part now needs to be replaced.
 - c. Load testing was not done.

Hitachi Storage Area Network (SAN)

During the site visit of the City Hall Data Center it was noted that there was a Hitachi SAN data backup system that was not being used. The City ultimately spent over \$500,000 on this system and we were told it was non-functional. This appeared to be a questionable purchase and resulted in a special investigation.

Results of this investigation are documented in a separate report to the City Manager, and to the City Finance Director as the interim supervisor of ITT to determine proper action. As this information is not

considered confidential the results will also be provided to the Audit Committee, and the Governing Body, in regular session, and to the Independent Public Accountant in accordance with governmental auditing standards.

Data Backup and Disaster Recovery

Backup of I-Series Financial Data

Per discussion with the Caryn Fiorina, Systems and Program Manager, ITT, the City currently uses an I-Series for its financial systems. **Note:** The I-Series was formerly referred to as the AS-400 financial system.

The I-Series currently houses:

1. Enterprise 1 Financials.
2. UCIS – Utility Information Water Refuse Utility Customer Information System (UCIS).
3. Sun Gard Community Development Applications,
 - a. Land Use,
 - b. Building Permits,
 - c. Business Licensing,
 - d. Code Enforcement.
4. Right now there are 4 LPARs²,
 - a. World LPAR – UCIS and SunGard applications,
 - b. Production LPAR – Enterprise 1 Production,
 - c. Web LPAR - which has the City's web application, this is the web server for the City's financials,
 - d. Test LPAR – Enterprise 1 test environment.

Tape Backups of Financial Data

Tape backups are done at City Hall where the I-Series financial system is located.

1. Daily - Data and objects are backed up on all 4 LPARS:
 - a. Daily backups are run Monday through Thursday,
 - b. Tapes are loaded by ITT personnel,
 - c. Backup is automated and runs at 11:55pm,
 - d. Daily backups are saved for a four month time span.
2. Weekly – A full systems save is done on all 4 LPARS:
 - a. The weekly system saves are run on Friday nights,
 - b. Tapes are loaded and initialized by ITT personnel, Employee 1,
 - c. A system shutdown must occur prior to backing up the tapes,

² LPAR – a logical partition (LPAR) is the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources can be operated independently with its own operating system instance and application.

- i. System shutdown is done remotely by a ITT Employee 2, this shutdown is done in a very precise order,
- d. Once confirmation is received that the systems are completely shut down back-up is initiated by Employee 1,
- e. Weekly backups are saved for 6 months,
- f. An annual backup is done on June 30th.

The daily and weekly back-up tapes are stored offsite. The daily backup tapes are stored in a cubicle which is behind a keyed entry door. The weekly systems saves are locked in Employee 1's office.

During the walkthrough of the data center it was observed that an error message appears that states "the daily saves are incomplete or are not successful". This was occurring on all 4 LPARs **(See Finding 6), (See Appendix Pictures - #7a through 7d)**.

Regarding the error message for unsuccessful backups Ms. Fiorina stated that "The reason we are getting this error is because the daily save was not able to save certain objects. The backup is saving all our data libraries successfully. The objects that are not being saved are logs and journals. Marco had entered a support call with IBM to find if there was a way to exclude these objects from the save but has since been moved to work on the website." The Marco referred to in this quote is Marco De Waart, Network Specialist, ITT.

In a follow up with IBM, ITT was told that the error message was occurring because they are doing the backups in a non-restricted state. Therefore, any application that is open and running may not be saved fully. ITT is working to resolve this issue, but for now it remains an open item.

Ms. Fiorina confirmed that there are lots of billing issues with the Water Utility. For that reason she has made the decision to keep daily backups for a four month time span. She stated that 95% of the issues are related to user error. Based on historical precedence she believes that weekly backups of anything older than four months are adequate. When asked if she was meeting the City and State data retention requirements she suggested meeting after the audit to discuss this issue further. She also suggested including someone from legal in that discussion to ensure compliance with any specific laws and regulations **(See Finding 7)**.

No exceptions were noted on testing the restoration of the tape backups of the daily saves of financial data. However, the restoration of the weekly and annual saves could not be tested due to system constraints and capacity issues. In an email from the Ms. Fiorina dated 06/28/2013 she stated that "In July, we are scheduled to create a new test web Lpar (sic) and we will be performing a system restore to the new LPAR. If you would like to use that as your system restore test we would be happy to accommodate the system test for the audit." **(See Finding 7)**.

File Server Mirrored Backup

The City has entered into a reciprocal arrangement with the Regional Emergency Command Center (RECC) to have a mirrored backup of the I-Series financial servers at their data center in exchange for them having a mirrored backup at a City data center. It should be noted that the server the mirrored

backup is housed on is owned by RECC, and at this time the City is not hosting a mirrored backup of RECC data. Access to the server room at RECC is restricted. Three of the four LPARs that reside at City Hall are replicated at RECC, they are:

- 1) World LPAR
- 2) Production LPAR – Enterprise 1 Production
- 3) Web LPAR

The Test LPAR residing at City Hall is not replicated at RECC.

The City has been replicating data at the RECC site for approximately 1 ½ to 2 years. To get a level of comfort that the system is replicating at 100% they use an iTera application as a tool for monitoring and reporting data replication for disaster recovery purposes. In order to fully test the system capabilities a roll swap needs to occur where one system switches off and the other switches on. ITT is in the process of negotiating a contract with Vision Solutions - iTera to test the mirrored site by doing a roll swap. At the time of this report, a roll swap has not occurred and the full capabilities of the mirrored backup have not been tested (**See Finding 7**).

Tape Backup of Email, Word, Excel, and Share Drive Documents

The City has a robotic tape backup that holds 32 tapes with 800 to 900 compressed gigabytes. The City uses a product called Backup Executive Software. This software enables the City to:

- Point to the servers to include in backup,
- Install remote software that shuts down unneeded services and performs backups,
- Monitor backups by reviewing a screen that shows if backups ran or failed,
- There are 24 tapes in rotation (the other 8 tapes are not being used in rotation). That is there is 24 tapes available, plus 8 being used for other purposes which equals 32 tapes total.

Testing of Internal Controls as Identified By External Auditors

The objectives of this audit included testing of the internal controls identified the external financial auditors as asserted to by ITT management as being effective. Based on management's assertions there were no identified findings for ITT as a result of the 2012 financial audit. The objective of this audit is to test these controls to verify they exist, and to determine whether they are effective.

The testing of the following internal controls was included in this audit:

- 1) A management steering committee is responsible for reviewing and approving IT plans and priorities.
 - a) Results of internal audit test work indicate that there is no steering committee, **this control is not effective (See Finding 4)**.
- 2) ITT management conducts regular risk assessments and addresses noted risks appropriately.
 - a) Results of internal audit test work indicate that a formal risk assessment process is not currently in place. **This control is not effective (See Finding 4)**.
 - b) The risk assessment process is ad hoc and informal.
 - c) There is also no formal policy or procedure for doing a risk assessment. In an email dated May 17, 2013 the Mr. Williams stated he is in the process of drafting a risk assessment policy, the

email included an attachment. The attachment was a draft of a policy titled Risk Assessment. However, in reading the draft it was really for incident management. When asked about this he stated this was an error and that he will provide internal audit with a more current draft.

- 3) All outside service providers used by the entity are evaluated to determine those who provide material financial services that may impact controls.
 - a) Internal audit test work indicates that **this control is not effective (See Finding 4)**.
 - b) According to the external financial auditor a relevant example of this type of provider would be the administrator of the City's (sic) Health Plan. When asked for clarification of this control he states that "The controls of the outside service provider may impact the City's IC system where the outside service provider provides significant financial services to the City. Common examples are an outside payroll contractor or processing of transactions in the case of financial institutions, calculation of depreciation and maintenance of capital assets, or administration of insurance or self-insured (sic) functions such as CSSF health plan (this one is relevant)."
 - c) Per an email from Thomas Williams dated 05/17/2013 "We're not doing anything along those lines." According to this email no documentation of the internal controls of the outside service providers is being done at this time. Mr. Williams is beginning the process of identifying these providers.
- 4) A backup and data retention policy/schedule exists, specifying how often backups are to be performed, how long they are to be retained, and where the backup media are to be stored.
 - a) Internal audit test work indicates that although a backup schedule exists, there is no current formal policy. **This control is not effective (See Finding 5)**.
 - b) The external financial auditor cites "IT policies appear to be outdated" in the 2009 Comprehensive Annual Financial Report (CAFR).
 - c) The external financial auditor cites "IT policies appear to be outdated" in the 2010 CAFR.
 - d) The external financial auditor does not cite this as a finding in either 2011 or 2012, although, policies are still not formalized or updated.
 - e) The external financial auditor indicates that this control does not exist, and is not effective, but did not cite it as a finding as the following was noted "There is a backup and retention policy for all financial system servers. Nightly program saves and weekly system backups, backups taken to Siringo location weekly for storage. Expected to complete in early summer locating critical networking to Century Link data center (Tier 3 or 4), should have a SOC1. Will also have a backup center at state ISD (probably a secondary location). Have a draft disaster recovery policy that is not yet finalized"
 - f) The referenced backup and retention policy is a draft. The 'draft policy' that was provided for data backups was at least 6 years old as it references the Net Apps data backup system that was replaced with the purchase of the Hitachi SAN system in 2007. The referenced backup schedules do exist, but are not part of a formal policy. Also, backup procedures for the I-Series financial data do exist, but are not formalized in a policy. Other policies/procedures are ad hoc and informal. A formal, current backup policy needs to be created. A formal disaster recovery and business continuity policy needs to be created.

- 5) Application data backups are performed to minimize the risk of lost or corrupted data. Backup tapes or other media are secure (accessible only by authorized personnel).
 - a) **This control is effective.**
- 6) Application data recovery procedures are tested at least once annually to ensure data integrity and recovery.
 - a) **This control is effective.**
- 7) File server backups are performed to minimize the risk of lost or corrupted data. Backup tapes or other media are secure (accessible only by authorized personnel).
 - a) **This control is effective for the financial servers,**
 - b) **This control is not effective for the non-financial servers (See Finding 8).**
 - i) The Hitachi SAN units were purchased for this purpose in 2007, but are not functional.
- 8) File server recovery procedures are tested at least once annually to ensure data integrity and recovery.
 - a) Internal audit test work indicates that **this control is not effective (See Finding 7).**
 - b) The external financial auditor cited this as a finding in 2009 in the CAFR.
 - c) The external financial auditor cited this as a finding in the 2010 CAFR.
 - d) The external financial auditor cited this as a finding in the 2011 CAFR.
 - e) The external financial auditor did not cite this as a finding in the 2012 CAFR.
 - f) Internal audit test work indicates that recovery attempts are ad hoc and informal, for the financial data, and that recovery is done on a crisis basis. A formal, annual, testing process needs to be implemented to ensure completeness and integrity of data.
 - g) The Hitachi SAN system purchased in 2007 to provide redundant back-up for nonfinancial data, was initialized to begin doing backups in late May 2013.
 - i) In an update from the William Smith, Network Operations Manager, ITT, he states that:

“These are the milestones and their dates that I consider to be key:

 - We completed the SAN configuration around May 10th. At that point, it was utilizable as a storage medium.
 - We completed the DFS configuration and started replicating files around May 16th.
 - DFS synchronization of the “Departmental Shares” completed on May 21st.
 - DFS synchronization of the “User’s My Documents Shares” completed on June 6th.”
 - h) Currently, a mirrored back-up is set up at the RECC for three of four LPARs for the iSeries financial data. A formal test involving a roll swap has never been done to assure the completeness and integrity of the data. ITT is in the process of setting up a formal testing procedure with a third party service provider.
 - i) Internal audit was unable to do 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.

- j) File server recovery is not effective for non-financial server backup as the servers were not functional.
- 9) Appropriate environmental controls exist to ensure the security and reliability of equipment in data centers and other technical facilities. Such controls include fire/smoke detection and fire suppression, temperature and humidity controls, and an uninterruptible power supply and/or backup generators where required.
- a) Internal audit test work indicates **these controls are not effective (See Findings 1 and 2)**.
- 10) An information security policy exists that defines information security objectives. This policy is supported by documents standards and procedures where necessary.
- a) Internal audit test work indicates this control is **not effective (See Finding 5)**.
 - b) The external financial auditor cites "IT policies appear to be outdated" in the 2009 CAFR.
 - c) The external financial auditor cites "IT policies appear to be outdated" in the 2010 CAFR.
 - d) The external financial auditor does not cite this as a finding in either 2011 or 2012, although, policies are still not formalized or updated.
 - e) ITT has been cited in the last two US Department of Transportation Financial Management Oversight (FMO) reports dated July 2012 and March 2013 for "Lack of a Comprehensive IT Policies and Procedures Manual". They have characterized this finding as a significant deficiency. The original recommendation was to "prepare a comprehensive Information Technology Security Policies and Procedures Manual." The current status states that "The Grantee indicated that it was still in the process of updating its policies and procedures. Draft versions of the updated IT policies and procedures were provided that addressed some of the areas noted in the findings including access to the data center, and the terminated employees system access policy. The Grantee did not have any documentation to show that it had established a policy to address areas such as risk assessment, incident response, or security awareness. Current procedures are not adequate. This finding is still applicable."
- 11) Physical access to computer room, file/communication servers, off-line data storage, and other sensitive storage is appropriately restricted to authorized personnel. Access is reviewed for appropriateness on a periodic basis.
- a) Internal audit test work indicates this control is not effective **(See Finding 3)**.

FINDING 1

Lack of environmental controls in data centers

Condition

During the walkthrough phase of this audit several internal control deficiencies regarding the environment in the data centers were noted, including:

- 1) The temperature in the City Hall data center / server room was 81 degrees on the day of the walkthrough,
 - a. Cooling unit in the City Hall data center is not receiving routine maintenance by a technician certified on these types of units.
- 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.
- 3) None of the three data centers (SFPD, City Hall, and Communications Room) has fire suppression, although, hand held chemical extinguishers are available.
- 4) Wiring in the City Hall data center is not protected from fraying on edges of raceway / rack and poses a fire risk **(See Appendix – Pictures #5)**.
- 5) There was significant clutter comprised of combustible material in the Communications Room, which is a fire code violation **(See Appendix – Pictures #1)**.
- 6) The three phase main feed in the Communications Room does not have a protective cover and poses a fire risk **(See Appendix – Pictures #4)**.

Criteria

Appropriate environmental controls should exist to ensure the security and reliability of equipment in data centers and other technical facilities. Such controls include fire/smoke detection and fire suppression, temperature and humidity controls, and an uninterruptible power supply and/or backup generators where required.

Cause

Internal controls pertaining to physical environment in the City's data centers are not effective. These deficiencies in the internal control environment can affect operations of the City. The specific internal controls deficiencies are 1) lack of a redundant cooling unit for the City Hall data center, 2) lack of water sensors or monitoring devices for flooding, 3) lack of fire suppression, and 4) lack of controls for fire prevention.

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. 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.

Another, less obvious risk is heat. 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, 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 down the road. Since the financial, email and network servers are all located in this room this is a critical issue. 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

The ITT department is evaluating the cost/benefit of moving the data center to a hosted site. Whether or not the entire data center moves, if there are any remaining servers the following considerations need to be made:

- 1) The cooling system needs to be evaluated for capacity issues, and needs to have proper, routine maintenance done by internal or external specialists familiar with and certified on this type of unit.
- 2) Flood detection devices need to be added under the raised floors, and monitored.
- 3) A fire suppression system needs to be evaluated.
 - a. Consider adding fire caulking to the Communications Room to make it a two hour fire rated room.
- 4) A protective fire resistant barrier needs to be placed between the wiring and the raceway/rack at the edge.
- 5) Remove clutter and other combustible materials from the server rooms. Yellow tape can be used to clearly mark areas in front of fire alarms and panels that need to be free of clutter.
- 6) A protective fire resistant cover needs to be placed over the three phase main feed.

Estimates for these improvements need to be provided so that senior management can better assess the cost of the improvements versus the current risk.

Management's Response and Implementation Date

ITT Management has met with Facilities Division Management on this issue. ITT Management also met with M&E Engineering, a local full service mechanical, electrical and fire protection engineering firm, to conduct an assessment of the Server Room environment. M&E believes that the AC unit is adequately sized, but recommends that a standby AC unit be installed. They also recommended that the AC units be placed on a quarterly preventive maintenance schedule and that automated fire suppression and moisture detection systems be installed. Of note is the fact that not having automated fire suppression systems in the data centers does not violate any fire code. Additionally, per the City of Santa Fe's Fire

Marshall, the Communications Room could be retrofitted to make it a two hour fire room in lieu of installing an automated fire suppression system. Nevertheless, the following are estimates for the systems recommended by M&E:

Standby AC Unit – City Hall Data Center - \$30,000 - \$40,000 **(90 days)**

AC Preventive Maintenance – City Hall Data Center \$1,500 - \$2,000 annually **(45 days)**

Moisture Detection & Alarm System – Police Department & Communications Room - \$6,500 - \$10,000 each **(90 days)**.

Fire Suppression System – City Hall, Police Department & Communications Room - \$12,000 each **(90 days)**

ITT Management has remediated this finding by having staff place nylon material under the cables to eliminate the potential for fraying edges that cause a fire risk. Nevertheless, a proposal has been obtained for a waterfall cabling system that will provide a more permanent solution that will also provide for more efficient cable management and ease of troubleshooting. This system is approximately \$4,000. The system will be installed in-house by ITT technicians. Clutter – ITT Management has remediated this finding by having staff remove the clutter and relocate boxed equipment from the Communications Room to eliminate the fire risk.

Protective Cover on Three Phase Main Feed –The Facilities Division has notified ITT that the electrical code does not permit them to modify this main feed panel by placing a protective cover over it. Alternatively, Facilities recommends that safety striping be placed on the floor in front of the main feed, advising not to stand or store materials within 3 feet of the main feed. ITT Management is requesting quotes for this striping and will order and install it as soon as possible. ITT Management estimates that this finding will be remediated within 15 days at a cost less than \$100.

The above recommendations are summarized below by priority:

<u>Data Center Priority</u>	<u>Remediation Option 1</u>	<u>Estimated Cost</u>	<u>Estimated Timeline</u>
City Hall	New Standby AC Unit	\$40,000.00	90 Days
	AC Preventative Maintenance	\$2,000 (annually)	45 Days
	Fire Suppression System	\$12,000.00	90 Days
Communication Room	Moisture Detection & Alarm System	\$10,000.00	90 Days
	Fire Suppression System	\$12,000.00	90 Days
Police Department	Moisture Detection & Alarm System	\$10,000.00	90 Days
	Fire Suppression System	\$12,000.00	90 Days

Alternately, if ITT management did nothing:

<u>Data Center Priority</u>	<u>Remediation Option 2</u>	<u>Remediation Option 2</u>	<u>Estimated Cost</u>	<u>Estimated Timeline</u>
City Hall	New Standby AC Unit	None	N/A	N/A
	AC Preventative Maintenance	None	N/A	N/A
	Fire Suppression System	Handheld Chemical Extinguisher (current)	\$0.00	N/A
Communication Room	Moisture Detection & Alarm System	Do Nothing	\$0.00	N/A
	Fire Suppression System	Handheld Chemical Extinguisher (current)	\$0.00	N/A
Police Department	Moisture Detection & Alarm System	Do Nothing	\$0.00	N/A
	Fire Suppression System	Handheld Chemical Extinguisher (current)	\$0.00	N/A

As indicated in the Finding Recommendation, the ITT Division is currently evaluating the cost/benefit of relocating the data center to a hosted site. This evaluation should be completed by September 2013. At that time a decision will be made to either relocate the Data Center including recommendations for appropriate system upgrades for remaining equipment, or to upgrade the existing Data Center systems with sufficient capacity for all equipment. Nevertheless, it is anticipated that the existing data centers will continue to house some equipment, and will therefore require all systems identified in the audit findings. ITT Management will request required funds in the form of a budget increase for current FY 13-14 budget no later than August 16, 2013. If not approved, ITT Management will make another request at the FY 13-14 Mid-Year Budget Review. ITT Management estimates that all required work could be completed within **90 days** after approval of funds and selection of a vendor; with consideration for appropriate approval through the procurement and committee approval processes.

Evaluation of Management's Response

Management's response is adequate. The prioritization of costs will help senior management and the governing body to determine the best use of financial resources. The prioritization list is in line with the potential risks. It is feasible to implement the highest priorities initially, and address lesser concerns at a later time.

FINDING 2

During the walkthrough phase of this audit several internal control deficiencies regarding the redundant power supply in the data centers were noted, including:

- 1) Lack of a back-up generator for 2 of 3 data centers.
- 2) Lack of routine maintenance on back-up generator at SFPD.
- 3) Lack of routine maintenance on the Uninterruptable Power Supply (UPS) at 3 of 3 data centers,
 - a. The City Hall data center was receiving routine maintenance through June 30, 2012. The UPS in both the City Hall Communications Room and SFPD have never had routine maintenance.

Condition

- 1) There is no backup generator at City Hall. This affects both the City Hall data center and the Communication's Room.
- 2) The backup generator at SFPD is not receiving routine maintenance.
 - a. In an effort to maintain a flat budget, the City opted to begin providing maintenance to the generator in-house.
 - b. On 06/21/2013 the Facilities and Evidence Manager at SFPD, stated that Fleet Management came out to service the generator and damaged it. He further stated that a radiator hose had cracked and needed to be replaced. The water was drained out of the generator so that they could replace the hose, but the heat pump was not turned off and ended up burning up. This part now needs to be replaced.
 - c. Load testing was not done.
- 3) The UPS units at SFPD, City Hall data center and the communication's room are not receiving routine maintenance.

Criteria

Appropriate environmental controls should exist to ensure the security and reliability of equipment in data centers and other technical facilities. Such controls include an uninterruptible power supply and/or backup generators where required.

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 effective. These deficiencies in the internal control environment can affect operations of the City.

Effect

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

A UPS is typically used to supply temporary power to critical applications and servers in the event of a power failure. There can be one or many in a datacenter. A UPS differs from an auxiliary or emergency power system or a standby generator in that it will provide near-instantaneous protection from input power interruptions by supplying energy stored in batteries or a flywheel. The on-battery runtime of most UPS sources is relatively short (typically, up to 45 minutes) but is sufficient time to start a standby power source or to properly shut down the protected equipment. If the UPS is not functioning properly IT systems may not be protected from the effects of power outages or fluctuations in electricity.

If there is a power failure at City Hall that lasts longer than the 30 to 45 minute cushion provided by the UPS City operations that flow through the City Hall data center or communication's room are at risk of shutting down. This includes, but is not limited to financial operations, network activity, and email. In addition, the 911 emergency locator database would be inaccessible.

Also, it should be noted that City calls routed to the Regional Emergency Command Center (RECC) first go through the City data center as the initial entry point. A shutdown of the City Hall data center could affect emergency response. For example, Fire and Police mobile units would not be able to connect back to RECC, but would have to revert to manual communications. This especially impacts public safety as the Fire Department uploads vital signs to a mobile unit which then gets loaded to dispatch. The ability for Police to enter a driver's information and get immediate feedback or further updates on calls, would be impacted as well as the ability to place an Amber Alert on a missing child.

A power failure affecting the City Hall data center would also impact other City services including, but not limited to senior services, library services, and the recreation centers which would lose their ability to function at point of sale/membership terminals, etc.

Recommendation

The ITT department is evaluating the cost/benefit of moving the data center to a hosted site. Whether or not the entire data center moves, if there are any remaining servers:

- 1) The UPS units at all three sites need to be evaluated for load capacity, and routine maintenance needs to be done either internally or externally by qualified technicians.
- 2) The backup generator at SFPD needs to have proper, routine maintenance done by internal or external specialists familiar with and certified on generators.
- 3) Estimates of the cost of a backup generator for City Hall need to be provided so that senior management can better assess the current risk versus the cost of the improvement.

Management's Response and Implementation Date

ITT Management has received estimates for a back-up generator at City Hall (alternatively a mobile back-up generator), and a preventative maintenance schedule for the generator at the Police Department (also the Radio Communications Prime Site). Proposals have also been solicited for preventative maintenance on the UPS systems at the Police Department and the Communications Room. The City Hall Data Center UPS is currently under a maintenance agreement and is in the process of being extended through 06/30/14. The following are estimates for these systems:

- Back-Up Generator for City Hall Data Center & Communications Room - \$100,000 **(120 days)**
- Mobile back-up generator for City Hall Data Center & Communications Room - \$55,000 **(90 days)**
- Preventative Maintenance for SFPD back-up generator **(30 days)**

In speaking with Eric Armstrong (BDD) and Joe Encinias (Fleet), they have agreed to perform necessary repairs (heater) and preventative maintenance on the back-up generator at the Police Department (PD). PD has ordered the heater repair equipment, and should receive it next week. Mr. Armstrong will schedule the repair work and train Fleet on the preventive maintenance soon after the equipment arrives. This should be completed NLT 08/16/13. Mr. Armstrong is a certified Emergency Power Systems Technician, and will train Fleet to perform the annual preventive maintenance on the system. Mr. Armstrong also recommends that an annual load bank test be performed on the unit. However, he would have to perform this test himself but does not have the load bank equipment to perform the test. To purchase a load bank would cost in the range of \$8,000 - \$10,000, which would have an ROI of 13-16 years in comparison to having an external firm do the preventive maintenance and load bank test (approximately \$600 annually). Therefore, ITT will contract with an outside firm to conduct the annual load bank test.

- Preventative Maintenance for Communications Room and SFPD UPS systems – **(30 days)**

At this point, Eric Armstrong, BDD, is willing to consider training ITT technicians to perform preventative maintenance on the UPS systems for the Communications Room and the PD Data Center. These UPS's are smaller systems that won't require much maintenance. Each of these systems could be replaced for an approximate cost of less than \$3,000 each; with annual battery replacements of less than \$200 each if required. The City Hall Data Center UPS is a larger more complex UPS that will remain under APC preventative maintenance at an annual cost of \$4303.19, which is currently in the ITT Budget. Mr. Armstrong and I will meet later this week or early next week regarding a training and preventive maintenance schedule. I anticipate that the first training and preventive maintenance (battery replacement if required) on these two UPS systems will be complete no later than 08/30/13.

Evaluation of Management's Response

Management's response is adequate. ITT management is looking first to an internal solution which maximizes the use of existing resources for on-going maintenance. This is a viable, strong, long-term

solution for on-going maintenance. Also, providing estimates for a backup generator and mobile backup generator will help senior management make decisions weighing the cost against the potential risk.

FINDING 3

Lack of adequate physical security in the data centers

Condition

- 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.
- 2) Physical access to the server rooms is not always restricted to authorized personnel, and is not reviewed on a periodic basis.
 - a. At the time of this audit vendors were not required to fill out user authorization forms to gain access to the data center.
 - b. 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.

Criteria

Physical access to computer room, file/communication servers, off-line data storage, and other sensitive storage should be appropriately restricted to authorized personnel. Access is reviewed for appropriateness on a periodic basis.

Cause

Internal controls pertaining to physical security in the City's data centers are not effective. These deficiencies in the internal control environment can affect operations of the City.

Effect

Not restricting access to who can enter a data center can result in an intentional or unintentional loss of data, or server downtime.

The ITT office is a barrier to the City Hall data center. Having this door left opened created the following risks:

- 1) Entry to the data center was possible given current vulnerabilities.
- 2) Additional strain was put on the cooling system as cool air was not contained. This was especially critical that weekend (Friday - March 8th to Monday - March 11th) as the temperature in the data center had been 81 degrees on Thursday, and was just starting to come down on Friday.
- 3) Computers and other assets stored in the ITT office were more susceptible to theft (**See Appendix - Pictures #6a, b, c**).

Recommendation

- 1) Ensure that doors to the data centers are locked at all times.
- 2) Ensure that only authorized personnel have access to the data centers.
 - a. If a key pad entry is used ensure that the key sequence is changed periodically to help prevent unauthorized access by past employees or by vendors who are no longer authorized to have access.
- 3) If swipe entry is used:
 - a. Disable swipe card when user no longer needs access.
- 4) Periodically review list of authorized personnel.

Management's Response and Implementation Date

ITT Management has reminded staff to ensure that the doors to the ITT Office at City Hall (office area leading to City Hall Data Center) and the Communications Room should be locked at all times when an ITT staff member is not present in those areas. The incident on 8/3/13, specified in the finding, concerning the ITT Office at City Hall was an isolated incident that management is confident will not happen again; nor has it happened since. However, the issue with the Communications Room is a reoccurring problem that is complicated by the fact that Facilities Division personnel also have the combination to the lock for this room in order to maintain electrical and other systems at City Hall. Remediation of this issue will require the cooperation of Facilities Division personnel. To this end, ITT Management has informed the Facilities Division Director, David Pfeiffer, about this issue; and he has agreed to cooperate and direct his staff to lock the room prior to leaving it unattended. Moreover, ITT Management has received an estimate for a key access system that would provide automated access control and electronic logs for City Hall Data Center (2 doors), City Hall Communications Room (1 door), Siringo Network Operations Center (2 doors), and Siringo ITT Admin (2 doors) in the amount of approximately \$10,500. ITT Management will request required funds in the form of a budget increase for the current FY 13-14 budget no later than July 31, 2013. If not approved, ITT Management will make another request at the FY 13-14 mid-year budget review. ITT Management estimates that the key access control system could be purchased and installed within **45 days** after approval of funds and selection of a vendor; with consideration for appropriate approval through the procurement and committee approval processes. When the system is upgraded it will provide for 1 year of access logs and 3rd party monitoring.

Additionally, a manual visitor access log and standard operating procedure will be implemented, and records will be maintained for 1 year. This log will be reviewed and filed electronically at the beginning of each month by the Network Operations Manager (Bill Smith). Only authorized ITT personnel will be assigned electronic keys, which will be disabled as soon as possible upon notice of assignment change that no longer requires access to controlled areas. Vendors and other visitors requiring access to these areas will be required to sign in using the manual visitor access log, and must be escorted by an authorized ITT staff person throughout the visit.

Evaluation of Management's Response

Management's response is adequate. It addresses the issue of the door being left unlocked and looks to a both a manual and automated long-term solution that would increase data center security. The solution includes estimates for implementing an automated solution that will help senior management weigh the costs against the potential risks.

FINDING 4

Lack of ITT entity level internal controls

Condition

The following deficiencies were found in regards to ITT entity level controls.

- 1) Lack of a steering committee.
- 2) Lack of a formal, annual risk assessment.
- 3) Not assessing the security environment and internal controls of outside service providers who provide significant financial services to the City.

Criteria

Internal controls are a combination of people, processes and tools that are put in place to prevent, detect or correct issues caused by unwanted events. The need is to create a carefully planned control framework that weaves the various types of controls together and protects the City from risks.

Entity level controls in ITT serve the purpose of providing direction and guidance to ITT and to senior management. A steering committee comprised of members from a cross section of senior management allows the ITT department to consider the timing of projects in order to maximize human and other ITT resources. Both the steering committee and the risk assessment process affect both short and long-term planning opportunities and enhance budgeting decisions.

- An ITT planning or steering committee should exist that reports to an appropriate level of senior management and includes representation from senior management, user management and the ITT function.
- IT management should conduct regular risk assessments and address noted risks appropriately. The risk assessment should be used for short and long-term planning purposes and to help make budgetary decisions.

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 ITT entity level activity are not effective. These deficiencies in the internal control environment can affect operations of the City.

Effect

Not having a steering committee or a formal risk assessment process to aid in short and long-term planning may result in an ineffective use of human and other resources and create bottlenecks when conflicting projects are competing for priority.

Not assessing the security and internal controls of outside service providers may result in unacceptable downtime to security breaches and loss of data and / or reputation to the City.

Recommendation

The City's senior management should appoint a planning or steering committee to oversee the IT function and its activities. Committee membership should include representatives from senior management, user management and the IT function. The committee should meet regularly and report to senior management.

A formal risk assessment process should be in place to help ITT management with their short and long-term planning process. A risk assessment is a tool to help focus attention to critical needs including, but not limited to use of technology, human resources, IT infrastructure, security threats, and legal and regulatory requirements.

Regarding outside service providers:

- Determine the City's major service providers.
- Assess the security and general control environment
- Determine that the provider develops and adheres to appropriate policies, procedures and standards.
- Rely on the work of their internal or external auditors if this assessment has been done through them,
 - If available, obtain a Service Organization Control report commonly referred to as an SSAE 16, SOC 1 or SOC 2.
 - SSAE 16 - Statement on Standards for Attestation Engagements number 16.
 - These reports document the results of the auditors test work regarding the security and internal control environment at the service provider's organization.

Management's Response and Implementation Date

ITT Steering Committee

Mr. Williams is collaborating with the Marcos Tapia, City Finance Director, on a formal resolution to establish an ITT Steering Committee. Mr. Tapia will take the lead on finding members of the Governing Body to support the resolution.

In anticipation of approval of the resolution, ITT Management has drafted governing documents for the ITT Steering Committee. These documents consist of a steering committee resolution, policy framework, and decision rights matrix.

The steering committee resolution is designed to provide the committee with formality in the areas of mission; membership; organizational structure; major responsibilities governance; organizational reporting relationship; authority; meeting requirements; work plans; and goals.

The policy framework provides formal policies in the areas of new initiative approval; approved funding models; review of existing initiatives; and reporting & tracking requirements for existing initiatives.

The decision rights matrix provides a summarized view of the decision-making authority of members within the committee.

ITT Management estimates that a functioning ITT Steering Committee could be in place with all required work documents approved within 30 days after City Council approval of a resolution to establish it.

Risk Assessment

ITT Management is currently drafting a Risk Assessment Policy that will outline a formal Risk Assessment Process. This policy will specify that risk assessments shall be performed on all key technological systems that house or access City of Santa Fe data. These assessments will address unauthorized access, disaster recovery, disruption, modification and destruction. The assessments will also identify known potential threats, likelihood of occurrence, and the magnitude of the impact of those threats should they occur. The policy will also specify that risk assessments shall be performed upon initial acquisition of key technological systems, or prior to the execution of service agreements whereby third party service providers maintain these systems on the City's behalf. Moreover, the policy will specify that all assessments be reviewed and modified as needed on an annual basis. ITT Management will submit a Risk Assessment Policy for approval within **90 days**. **(See Management Response in Finding 5)**.

ITT has scheduled an upgrade to the OS400 Operating System for the iSeries for late 2013 (probably November 2013). This upgrade will provide a good opportunity to test a new Risk Assessment Policy. The Risk Assessment will be done in September (to allow time for the policy to be approved), and would include ITT and Finance. The results will be utilized to modify the implementation tasks in order to mitigate the identified risks.

Outside Service Providers

ITT Management is in the process of researching and drafting a policy to satisfy this control. To date, we have been unable to locate a policy example despite inquiries with Gartner and other organizations. Nevertheless, an appropriate policy framework appears to include 1) determine which outside service providers provide key financial services to the City 2) determine the security and control environment for the providers 3) request SSAE 16 SOC 1 or SOC 2 for providers, and 4) include requirement in all service agreements.

ITT Management will submit this policy for approval within **45 days** with consideration for collaboration with Finance Department staff to determine which providers provide key financial services to the City, determine the security and control environments for these providers, request SSAE 16 SOC 1 or SOC 2, and modify future service agreements for these providers accordingly.

Evaluation of Management's Response

ITT Steering Committee

Management's response regarding a steering committee is adequate. Involving the City Finance Director will help to ensure a committed involvement of any personnel participating on the committee that report through finance. Formalizing the committee in a resolution will help impart the significance of this committee, and creating documents to provide guidance will give the needed direction.

Risk Assessment

Management's response is marginally adequate. It is acceptable that ITT management is taking responsibility and has agreed to create a formal risk assessment process, and will be testing it in September. However, findings regarding lack of ITT policies have been cited for years, and each time there is a promise of a deliverable that is never met. In order for this response to be adequate there has to be accountability if the deliverable is not met.

Outside Service Providers

Management's response is adequate. Collaborating with the finance department to obtain a list of relevant service providers and obtaining a Statement of Standards on Attestation Engagements (SSAE) Service Organization Control (SOC) Type 1 or Type 2 report from each of them will address this finding. The purpose of an SOC 1 or SOC 2 is to provide assurance that the entity has been audited and their basic internal controls over financial reporting are adequate. This solution leverages off of the work of the entities auditors. This is a low cost solution that delivers high results. Also, requiring future service agreements to state that an SSAE SOC 1 or 2 is required to do business will provide assurance on future contracts.

FINDING 5

Lack of formal policies and procedures

Condition

The following was noted regarding ITT policies and procedures:

- 1) Risk assessment - There is no formal, annual risk assessment process, and there are no formal policies and procedures regarding the risk assessment process.
- 2) Back-up and data retention
 - a. 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.
 - b. Also, retention of backups does not take into account City or State data retention requirements.
- 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 is in process is no longer an acceptable response.

- a. The external financial auditor cites “IT policies appear to be outdated” in the 2009 CAFR.
- b. The external financial auditor cites “IT policies appear to be outdated” in the 2010 CAFR.
- c. ITT has been cited in the last two US Department of Transportation Financial Management Oversight reports dated July 2012 and March 2013 for “Lack of a Comprehensive IT Policies and Procedures Manual”. They have characterized this finding as a significant deficiency. The original recommendation was to “prepare a comprehensive Information Technology Security Policies and Procedures Manual.” The current status states that “The Grantee indicated that it was still in the process of updating its policies and procedures. Draft versions of the updated IT policies and procedures were provided that addressed some of the areas noted in the findings including access to the data center, and the terminated employee’s system access policy. The Grantee did not have any documentation to show that it had established a policy to address areas such as risk assessment, incident response, or security awareness. Current procedures are not adequate. This finding is still applicable.”

Criteria

Internal controls are a combination of people, processes and tools that are put in place to prevent, detect or correct issues caused by unwanted events. The need is to create a carefully planned control framework that weaves the various types of controls together and protects the City from risks.

Formal policies need to exist regarding:

- Risk assessment and prioritization and how this impacts short and long-term planning,
- Data back-up and disaster prevention and recovery, including
- ITT Security.

Cause

An internal control environment that is clearly defined in policies and procedures does not exist. This is creating a weak internal control environment which can affect operations of the City.

Effect

- 1) Not having a provision for a systematic risk assessment in line with control practices may result in missing opportunities for organizational synergy and avoidance of duplication of risk management effort gained through aligning the IT risk assessment framework with the broader corporate and IT governance process.
- 2) Not having formal policies creates a situation where each person may have a different understanding of how backups occur, what data is to be retained, and how it is to be recovered. Also, if a key person leaves, it creates a vulnerability that the procedures for a key process will leave with them.

- a. The City faces the following increased risks by not having a formal backup and data retention policy:
 - i. Legal and regulatory data retention requirements may not be met,
 - ii. Consistency with backup strategies may not be maintained,
 - iii. The business impact of system failures or disasters that result in the destruction of data may not be minimized,
 - iv. Incomplete, inaccurate and untimely recovery of data in the event of a system failure or disaster may occur.
- 3) Not having clearly defined security policies and procedures may result in:
 - a. Information systems that are not available and useable when required (availability),
 - b. Data and information that are not disclosed only to those who have a right to know it (confidentiality), and
 - c. Data and information that are not protected against unauthorized modifications (integrity).
 - d. *Most data and information in the City are not considered to be confidential due to the Inspection of Public Records Act (IPRA), but confidentiality does bear mentioning.***

Recommendation

As the City grows and the IT environment becomes more complex, it is of increasing importance to move to a more formal, controlled environment. Historically, it may have been efficient and effective to not have formalized policies and procedures in ITT. However, as the environment has become increasingly complex and the repercussions more severe, formality is no longer an option. ITT needs to formalize their policies and procedures. Backup policies and procedures need to take into account the legal and regulatory environment.

Management's Response and Implementation Date

The ITT Division Director, working in collaboration with the Network Operations Manager and Systems & Programming Manager, will submit formal policies for risk assessment, data back-up & disaster recovery, and a comprehensive security policy for approval within **90 days**.

Evaluation of Management's Response

Management's response is marginally adequate. It is acceptable that ITT management is taking responsibility and has agreed to submit formal policies for risk assessment, data back-up & disaster recovery, and a comprehensive security policy for approval within **90 days**. However, findings regarding lack of ITT policies have been cited for years, and each time there is a promise of a deliverable that is never met. In order for this response to be adequate there has to be accountability if the deliverable is not met.

FINDING 6

Daily saves of financial data are unsuccessful or incomplete **(See Appendix – Pictures #6)**

Condition

An error message stating the daily saves on the financial servers “are unsuccessful or incomplete” is occurring on all 4 LPARS.

In an email from Caryn Fiorina, Systems and Program Manager, ITT, dated 06/19/2013 she states that “the backup is saving all our data libraries successfully. The objects that are not being saved are logs and journals.” The problem with this is that an assumption is made that every time this message occurs it is only because non-essential logs and journals were not saved correctly. This might not always be a correct assumption.

In an email from Zeke Perea, Network Specialist, ITT, he states that the error message has been occurring for three to four years.

Criteria

In order for this internal control to operate as designed the message should state the save was complete and successful, unless there is a problem that ITT needs to be alerted to.

Cause

Error messages are an internal control designed to alert management of potentially serious issues. This internal control is ineffective as management is assuming the message always relates to non-essential objects such as logs and journals.

Effect

Assuming that the message is just referring to failed backups of unnecessary logs and journals may result in not actually knowing when a backup of critical financial data has failed and may result in a problem that is fairly easy to fix perpetuating itself day after day. The problem may not be recognized until a restore of the data fails.

Recommendation

Evaluate the steps necessary to remediate this issue, and resolve.

Management’s Response and Implementation Date

ITT Management has initiated a trouble resolution with IBM Technical Support regarding this issue. It should be noted that all objects in question are saved as part of the system save that occurs each week on Friday evenings. The primary question is whether or not the objects in question need to be saved on a daily basis as part of the daily save routine. If IBM recommends that these objects be saved daily, then the daily save routine will need to be modified to accommodate restricted state saves. The daily save routine does not currently run in a restricted state, because it is automated and unattended. In order to place the system in a restricted state (as is the case with system saves), daily saves would have to be attended (not automated). ITT also had a conference call with Mainline Information Systems (IBM Tech

Support) and Randy Peterson Consulting on 07/25/13 to discuss this issue in depth to determine an appropriate solution. The net recommendation from IBM Tech Support and the consultants was to remove the objects, which are part of the Integrated File System (IFS), from the daily save routine. These objects, and the IFS as a whole, are saved as part of the weekly system save. They do not change often enough to justify saving them on a daily basis. ITT Management removed these objects from the daily save routine on the WORLD LPAR for the 8/3/13 daily save; which ran successfully without exceptions. This adjustment will be implemented and tested for daily saves for all LPARs by 8/17/13. **15 days.**

Evaluation of Management's Response

Management's response is adequate.

FINDING 7

Lack of formal annual testing of file server back-ups and recovery procedures

Condition

- 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.
- 2) A formal annual testing of the file servers doing mirrored backup of the non-financial data is not being done.
- 3) Internal Audit was unable to do 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.
- 4) City and State data retention requirements for electronic data may not be retained for the appropriate time periods.

Criteria

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

Data retention, including retention of electronic data, needs to adhere to legal and regulatory requirements including City ordinances and NM State Statute 1.18.341, Executive Records Retention and Disposition Schedules.

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

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 is vulnerable to not being able to recover in the event of a disaster.

Recommendation

- 1) Continue contract negotiations with Vision Solutions - iTera to begin testing the mirrored backup at the RECC site.
- 2) Develop a plan for annual testing of financial and non-financial file server recovery.
- 3) Ensure that City and State data retention requirements adhere to legal and regulatory requirements.

Management's Response and Implementation Date

ITT Management currently has a negotiated engagement with Vision Solutions 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). Vision Solutions is finalizing City of Santa Fe business license requirements, and should be prepared to sign the Professional Services Agreement by August 31, 2013. ITT Management estimates that at least one virtual role swap and one live role swap will be conducted within **90 days**. These tests will be conducted on an annual basis, with test results maintained for not less than 36 months.

Moreover, the ITT Division Director, in collaboration with the Network Operations Manager and the Systems & Programming Manager will immediately begin drafting a formal data retention policy that is based upon City and State legal and regulatory requirements. The policy will specify data retention methods and data retention periods for iSeries data (AS400 or IBM System I) and open systems data (email and file servers); in addition to annual testing requirements. This finding will be remediated within **90 days**.

Evaluation of Management's Response

Management's response is adequate.

FINDING 8

File server backup is not occurring on non-financial data such as email, MS Word documents, Excel spreadsheets, and Share Drive documents.

Condition

The Hitachi SAN purchased in 2007 was intended to provide file server backup of non-financial data. The SAN was found to be non-functioning during the course of this audit.

Criteria

File server backup of non-financial data such as email, MS Word documents, Excel spreadsheets, and Share Drive documents needs to occur for disaster recovery purposes.

Cause

Failure to implement

Effect

The City is at risk in the event of disaster.

Recommendation

The Hitachi SAN units at the City Hall data center and the SFPD are at the end of their five year asset life. At end of life they will no longer be supported by either the hardware or software vendor. ITT management needs to assess how best to move forward to ensure the increasingly important redundant backup of its non-financial data.

Management's Response and Implementation Date

The City currently utilizes a combination of Tape backup and NAS (network attached storage) devices to regularly backup data assets that have been classified here as "non-financial data".

In this effort, the Hitachi WMS-100 and an associated server was set up as a DFS (distributed file system) mirror of the primary file server located at the City Hall datacenter, replicating it to the secondary datacenter located at the Police Department. This work was completed in early June 2013, and a real-time mirroring for departmental shares and user directories is in place. Additionally, Microsoft's DFS solution can be further leveraged to provide automatic "business continuance" access to this data in the event of failure.

Currently, ITT has added a second DFS server at the Police Department datacenter to accommodate additional server mirroring. This server was re-deployed using existing server assets. ITT will also relocate the Hitachi AMS-200 unit, which currently resides at the City Hall Data Center, to the police datacenter to provide additional data storage capacity. By having both SAN units located in the secondary site, geographical separation is achieved for a DR solution; and enough space to accommodate the Exchange email replicas that are planned for later this year (likely by October 2013).

Unfortunately, due to the deficiencies of both datacenter locations, the approaching end of available service for the Hitachi equipment, and the City's rapidly expanding storage needs, this solution should be considered only a stop-gap measure until a more appropriate disaster recovery environment can be realized. ITT Management has obtained a quote in the amount of approximately \$24,000 that would provide hardware maintenance for the Hitachi SAN equipment through 06/30/14 (02/28/14 for the Brocade switches). Placing the existing Hitachi SAN equipment back under maintenance will be considered as part of the cost-benefit analysis that will take place at the conclusion of the network and organizational assessment.

Evaluation of Management's Response

Management's response is adequate.

APPENDIX

Pictures

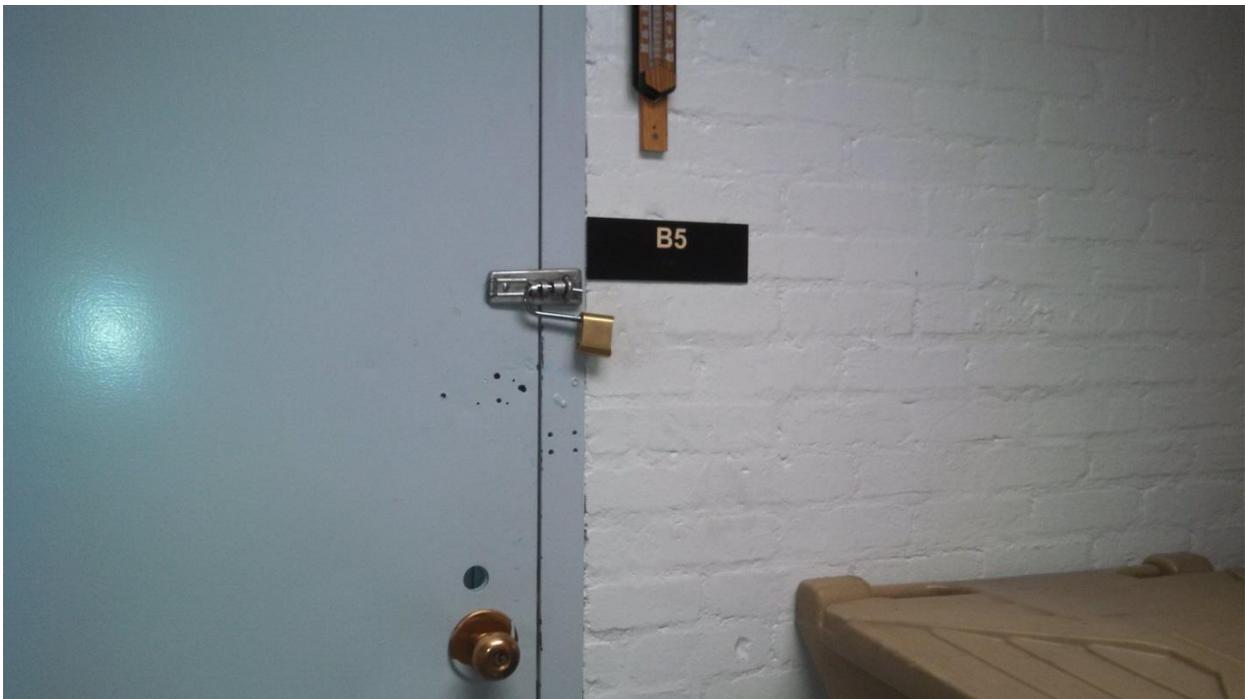
#1 - Combustible material in Communication's Room directly beneath the fire alarm.



#2 - Combustible material/clutter in Communication's Room



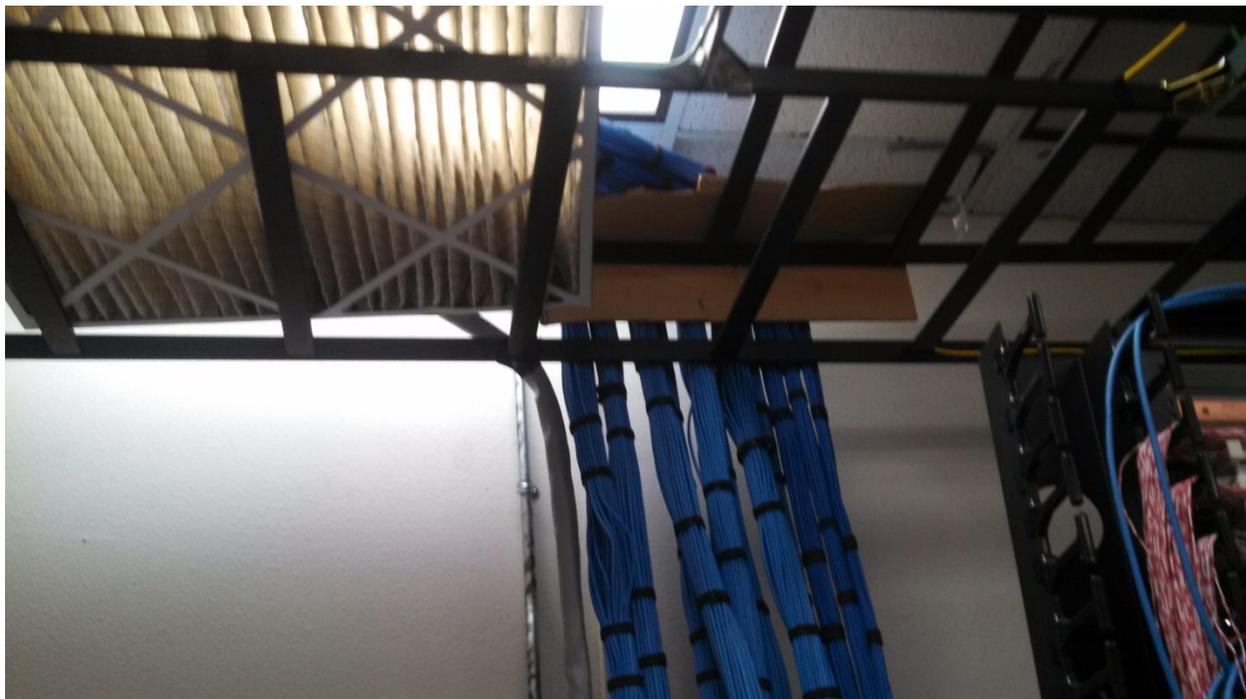
#3 - Unlocked door to Communication's room



#4 - Unprotected three phase power feed



#5 - Combustible material (cardboard) placed beneath power lines to protect them from fraying



#6a Computers and other equipment stored in City Hall Data Center – at risk due to open door.



#6b ITT assets at risk due to open door.



#6c More computer equipment stored in City Hall Data Center – at risk due to open door.



Data Back-up and Recovery

#7a Prod LPAR

Additional Message Information

```
. . . . : CPI1E62      Severity . . . . .
. . . . : Information
. . . . : 06/18/13      Time sent . . . . .

. : *DAILY backup not successful or not complete
. : The *DAILY backup ended with message CPF1EE7.
. : For more information, use the Display Job (DS
job log for job 289211/QSYSOPR/QEZBKTMMON.
```

o continue.

Print **F9**=Display message details **F12**=Cancel
istance level

```
Additional Message Information
. . . . . :      CPI1E62      Severity . . . . .
. . . . . :      Information
. . . . . :      06/18/13      Time sent . . . . .

. :      *DAILY backup not successful or not complete
. :      The *DAILY backup ended with message CPF1E68.
. :      For more information, use the Display Job (DS
job log for job 718236/QSYSOPR/QEZBKTMMON.

o continue.

Print      F9=Display message details      F12=Cancel
istance level

Online | | | | 1.1
```

```
Additional Message Information

. . . . : CPI1E62
. . . . : 06/18/13      Time sent . . . . .

. : *DAILY backup not successful or not complete

. : The *DAILY backup ended with message CPF1E68.
. : For more information, use the Display Job (DS
job log for job 585332/QSYSOPR/QEZBKTMMON.

) continue.

Exit  F6=Print  F9=Display message details  F12=C
istance level
on complete to the default printer device file.

Online  X-HELP  1,1
```

```
Additional Message Information

. . . . : CPI1E62
. . . . : 06/18/13      Time sent . . . . .

. : *DAILY backup not successful or not complete

. : The *DAILY backup ended with message CPF1E68.
. : For more information, use the Display Job (DS
job log for job 939071/QSYSOPR/QEZBKTMMON.

o continue.

Exit  F6=Print  F9=Display message details  F12=C
istance level

Online | | | | 1,1
```