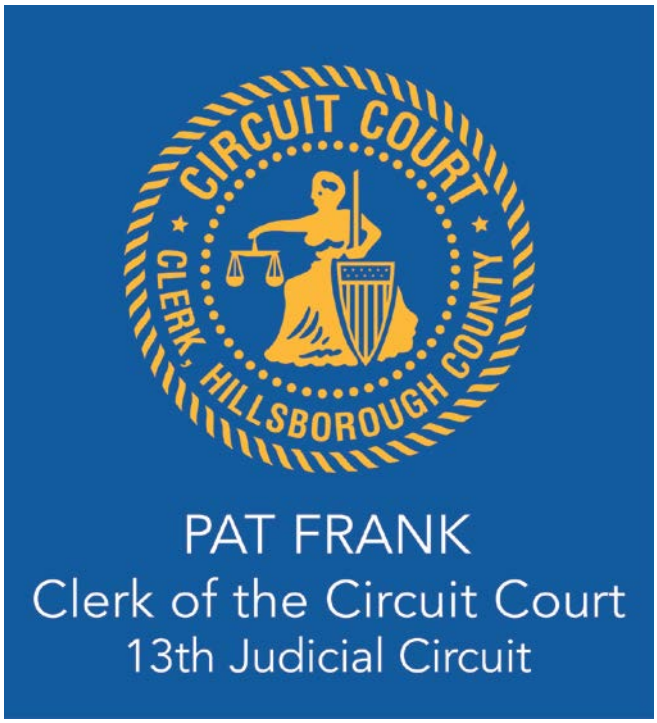

COUNTY AUDIT

HILLSBOROUGH COUNTY, FLORIDA

INFORMATION AND TECHNOLOGY SERVICES DEPARTMENT'S (ITS) PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS

REPORT # 268

NOVEMBER 13, 2014

PAT FRANK
Clerk of the Circuit Court
13th Judicial Circuit

November 13, 2014

The Honorable Kevin Beckner
The Honorable Victor D. Crist
The Honorable Ken Hagan
The Honorable Al Higginbotham
The Honorable Lesley "Les" Miller
The Honorable Sandra L. Murman
The Honorable Stacy White

Dear Commissioners:

The Audit Team performed an audit of the Information and Technology Services Department's (ITS) physical and environmental security controls (Audit Report # 268, dated November 13, 2014). Responses to the Audit Team's recommendations were received from the Director of the ITS and have been included in the Report after each audit comment and recommendation.

The purpose of this Report is to furnish management independent, objective analysis, recommendations, counsel, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

The Audit Team appreciates the cooperation and professional courtesies extended to the auditors by the Director and personnel of the ITS during this audit.

Sincerely,
Peggy Caskey, CIA, CISA, CFE
Director of County Audit

CC: Mike Merrill, County Administrator
Bonnie Wise, Chief Financial Administrator
Earl Williams, Director, Information and Technology Services
Bruce Dangremond, Performance Mgmt, Business and Support Services

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

The Information and Technology Services Department (ITS) has three main production equipment rooms which are maintained by the ITS Infrastructure and Telecommunications Services Area.

Two facilities contain servers, storage, and data backup systems supporting the production data processing and Internet connectivity needs of the County's wide area network.

Another facility houses servers, storage, and backup systems that support the production data processing and Internet connectivity needs for County employees during disaster recovery operations.

There are 22 additional remote server sites throughout Hillsborough County that are controlled by the ITS.

OBJECTIVE

Determine whether or not adequate and effective controls are in place to protect the environmental and physical security of information technology servers. Specifically:

- Determine if the ITS *Information Security Standards* (revised November 2011) adequately address physical and environmental server controls.
- Evaluate if physical and environmental security is in compliance with the ITS *Information Security Standards*.

SCOPE

The audit was conducted in accordance with the *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The Audit Team evaluated the ITS *Information Security Standards* against applicable *COBIT 4.1* control principles contained in the IT governance framework created by ISACA (an international professional association focused on information technology). The Audit Team: identified the population of servers; selected a

sample of server control environments for site visits; and compared actual practices to compliance with the ITS *Information Security Standards*.

The Audit Team's work was performed during the period of June – September 2014.

OVERALL EVALUATION

The ITS personnel were responsive to the Audit Team's inquires and provided data and other requested information in a prompt and courteous manner. The Audit Team found the ITS personnel to be knowledgeable and dedicated employees who were receptive to the Audit Team's suggestions for improvements.

AUDIT COMMENT	CONCLUSION OF OBJECTIVE	PAGE
1	The ITS developed *Information Security Standards* that adequately address physical and environmental security controls.	3
2	The ITS has reasonably mitigated the physical and environmental risks for the main server room locations and practices align with the ITS *Information Security Standards*.	6
3	Opportunities exist to enhance the physical and environmental security controls at remote server locations.	10

OPINION

The ITS developed *Information Security Standards* and implemented controls that provide a reasonable level of assurance that the physical and environmental risks to the ITS servers are effectively mitigated. The recommendations in this report represent opportunities to further strengthen the overall physical and environmental controls for the ITS server locations.

The exit conference was held on November 5, 2014.

Other minor concerns not included in this report, have been communicated to management and/or corrected during fieldwork.

AUDITED BY

Peggy Caskey, CIA, CISA, CFE, Director of County Audit
Mary Ann Kominsky, CIA, CISA, CPA, IT Audit Manager
Heidi Pinner, CIA, CFE, Senior Internal Auditor

AUDIT COMMENTS & RECOMMENDATIONS

AUDIT COMMENT 1

The ITS developed *Information Security Standards* that adequately address physical and environmental security controls.

To determine whether or not the ITS *Information Security Standards* include controls to adequately address the ITS physical and environmental server security, the Audit Team evaluated these Standards against the *COBIT 4.1* control framework: *12.3 Physical Security Measures, 12.4 Physical Access,* and *12.5 Protection Against Environmental Factors*. This testing was limited to evaluating the ITS *Information Security Standards* for completeness.

The ITS *Information Security Standards* substantially conform to the above referenced *COBIT 4.1* physical and environmental security control best practices. The Standards substantially address the key physical and environmental risks to the County's information technology servers. These include:

- Controlling physical access to the ITS server rooms, limiting disclosure of the server room locations, and establishing secure transport or removal of equipment.

- Requesting and granting user access to the server room locations, periodically reviewing user access rights, and regular training on physical security awareness.

- Establishing a risk assessment process to identify potential environmental threats to server equipment, requiring certain environmental controls for server rooms, and prohibiting eating, drinking and smoking in sensitive areas.

The Audit Team also identified a few control best practices which may be addressed by practice, but are not represented in the ITS *Information Security Standards*.

RECOMMENDATIONS

To establish the best practice activities into formal management directives, consideration should be given to incorporating the following additional physical and environmental security control objectives into the ITS *Information Security Standards:*

1. Periodically test and document the preventive, detective and corrective physical security measures to verify the adequacy of their design and the degree of implementation and effectiveness.

2. Define a process for recording, monitoring, managing, reporting and resolving physical security incidents, in line with the overall information technology incident management process.

3. Register all visitors, including contractors and vendors, to information technology sites. Define and implement a policy requiring visitors to be escorted by an ITS staff member when entering and exiting information technology sites and to be periodically monitored by an ITS staff member while on-site.

4. Prohibit storage of stationery and other supplies posing a fire hazard inside server room locations.

5. Ensure that particularly sensitive server locations are frequently evaluated (including weekends and holidays).

6. Include temperature and humidity control monitoring requirements.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

1. *ITS will test and document the preventative, detective and corrective physical security measures on a semi-annual basis.*

2. *ITS will include a process for recording, monitoring, managing, reporting and resolving physical security incidents in our existing security incident response plan.*

3. *For the ITS main computer rooms, visitors are currently required to register in a log book. For the remote sites ITS will inform the site managers of this*

requirement, provide a logging method for this purpose, and post a reminder sign on the server room entry door. ITS does not have the staffing required to escort visitors at all times while on-site and will accept the risk as additional staffing for this purpose would not be a prudent use of County's financial resources.

4. *For the three ITS main computer rooms, storage of stationary and other supplies posing a fire hazard is already prohibited and monitored. For remote server sites, ITS will inform the site managers of this requirement and post a reminder sign on the server room entry door.*

5. *ITS currently conducts a site inspection of particularly sensitive server locations on a quarterly basis and will begin quarterly evaluation of entry logs (including weekends and holidays) for those sites as well.*

6. *ITS' current policy is to monitor the ambient temperature of all server room locations. ITS will ensure temperature is monitored at all server locations and any deficiencies discovered will be resolved. ITS currently monitors and controls the humidity of the main server room locations. Humidity at remote site server locations is not monitored or controlled and management accepts the risk for those locations.*

TARGET COMPLETION DATE

1/31/15

AUDIT COMMENT 2

The ITS has reasonably mitigated the physical and environmental risks for the main server room locations and practices align with the ITS *Information Security Standards*.

The two main server room locations and the disaster recovery location were evaluated to determine whether or not controls adequately and effectively address physical and environmental security. The Audit Team based this evaluation on site visits, review of automated access rights and logs, and review of the process to grant and monitor the use of physical keys.

Overall, these three locations substantially comply with the ITS *Information Security Standards* and best practices associated with physical and environmental security controls. For example:

- Control mechanisms are in place to prevent unauthorized access.
- Directional signage does not indicate server room locations.
- Entry logs are secured, maintained and monitored periodically.
- Access rights are reviewed and updated regularly.
- Eating, drinking and smoking are prohibited in sensitive areas.
- Backup power supplies are utilized.
- Emergency power switches and emergency lighting are utilized.
- Server room doors automatically secure upon exit.
- Server rooms are clean and free of unnecessary clutter and debris.
- Locations are equipped with fire detection/suppression system(s) and inspections are up to date.
- Water, temperature and humidity sensors are installed and configured to alert the ITS staff members of undesirable environmental conditions.

The Audit Team also identified the following control areas where a physical or environmental security standard or best practice was not fully implemented:

1. Using intrusion detection alarms,
2. Limiting physical address disclosure for server room locations,
3. Monitoring all forms of server room access,
4. Testing backup power equipment, and
5. Testing the power down procedure.

Addressing these control opportunities will further enhance the physical and environmental security of the main server room locations and the disaster recovery location.

RECOMMENDATION

1. Consideration should be given to implementing intrusion detection controls for the main server room locations.

CLIENT RESPONSE

Management Accepts Risk

CORRECTIVE ACTION PLAN

ITS will rely on existing compensating controls, which reduce the risk of unauthorized entry to main server rooms. Main server rooms are in locations that have multiple layers of physical entry controls. An unauthorized person would have to successfully bypass these controls before reaching the server rooms.

TARGET COMPLETION DATE

N/A

RECOMMENDATION

2. Consideration should be given to limiting disclosure of the physical address of the server room locations.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will review documentation published on the County's Intranet site (i.e. COIN) and the County website. Any documentation containing server site addresses will be redacted or removed as appropriate.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

3. Consideration should be given to monitoring all forms of access to the main server room locations.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will research solutions for surveillance cameras to be placed at each main server room entrance and submit a Decision Unit for funding in FY16 or procure in FY15 if funding becomes available.

TARGET COMPLETION DATE

4/30/16

RECOMMENDATION

4. Consideration should be given to coordinating with the Facilities Department to monitor and test server room location's building generators.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

The Facilities Department will be contacted to request that their generator testing schedule for server room locations is provided to ITS.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

5. Consideration should be given to developing, and periodically testing, the process for an emergency shutdown of the main server room locations.

CLIENT RESPONSE

Management Accepts Risk

CORRECTIVE ACTION PLAN

ITS will document the process for an emergency shutdown of the main server room locations. The process will be tested during required shutdown events.

TARGET COMPLETION DATE

1/31/15

AUDIT COMMENT 3

Opportunities exist to enhance the physical and environmental security controls at remote server locations.

A sample of six remote server locations were evaluated to determine whether or not controls are in place to adequately and effectively address the physical and environmental security of the ITS servers. The Audit Team performed onsite visits and reviewed the process for accessing server room locations.

The six remote server locations tested incorporated and complied with many of the ITS *Information Security Standards* and best practices associated with physical and environmental security controls. The following controls were operating as designed:

- At least one control mechanism restricted access to the server locations.
- Directional signage did not indicate the physical address of any of the six locations.
- Backup power supplies were operational at each of the six locations.
- Remote server room doors automatically secured the six locations upon exit.
- Emergency lighting was operational in four locations.

The Audit Team observed several instances where the ITS *Information Security Standards* or best practice was not consistently applied:

1. Entry logs or visitor logs were not maintained at any of the six remote server room locations.
2. Eating, drinking and smoking were not specifically prohibited at any of the six locations and evidence of food consumption was present at one location.
3. Emergency power switches were available at two of the six locations.
4. Three of the six locations contained excessive clutter or debris.
5. Fire detection/suppression equipment was not present or was not current at three of the six locations.
6. Temperature and humidity sensors were not installed to alert the ITS staff members of undesirable environmental conditions at three of six locations.
7. Servers were observed beneath sprinkler systems or air conditioning units at three of the six locations.

The Audit Team acknowledges that the ITS' ability to implement some of these controls at remote server locations is limited by the facilities in which they are housed.

RECOMMENDATION

1. Consideration should be given to requiring and maintaining entry logs at remote server locations.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will inform the site managers of this requirement and provide a logging method for this purpose. Additionally, ITS will provide appropriate signage on server room entry doors.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

2. Consideration should be given to prohibiting eating, drinking and smoking within sensitive areas of remote server locations.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will inform remote site managers that eating, drinking and smoking within sensitive areas of remote server locations is prohibited. Additionally, ITS will provide appropriate signage on server room entry doors.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

3. Consideration should be given to ensuring that emergency power switches are installed at remote server locations as deemed necessary.

CLIENT RESPONSE

Management Accepts Risk

CORRECTIVE ACTION PLAN

In consideration of the cost vs. benefit, the installation of an emergency power switch would not be a prudent use of the County's financial resources.

TARGET COMPLETION DATE

N/A

RECOMMENDATION

4. Consideration should be given to ensuring that server rooms are free of excessive clutter or debris.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will inform remote site managers that server rooms must not be used as a storage area and must remain free of excessive clutter or debris.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

5. Consideration should be given to ensuring that fire detection and suppression equipment is present and current at each remote server location.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

ITS will inspect each remote server room location to ascertain if fire detection and suppression equipment is present. Any deficiencies will be addressed with the Facilities Department and/or the remote site managers.

TARGET COMPLETION DATE

3/31/15

RECOMMENDATION

6. Consideration should be given to ensuring that remote server locations are equipped with environmental sensors to alert the ITS of unfavorable conditions.

CLIENT RESPONSE

Management Accepts Risk

CORRECTIVE ACTION PLAN

ITS will ensure that remote server locations are equipped with temperature monitoring equipment.

TARGET COMPLETION DATE

1/31/15

RECOMMENDATION

7. Consideration should be given to ensuring that servers are not located directly under water pipes, sprinklers or air units.

CLIENT RESPONSE

Management Accepts Risk

CORRECTIVE ACTION PLAN

Due to physical space constraints at the remote sites and the costs associated with relocation and/or rerouting of space and/or infrastructure, these expenditures would not be a prudent use of the County's financial resources.

TARGET COMPLETION DATE

N/A