607

SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FROM: Auditor-Controller

SUBMITTAL DATE:
November 26, 2014

SUBJECT: Internal Audit Report 2013-011: Riverside County Information Technology. [All Districts][$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2013-011: Riverside County Information Technology

BACKGROUND:

Summary

The Internal Audit Division of the Auditor-Controller's Office has completed an audit of Riverside County Information Technology (RCIT). The audit objective is to provide management and the Board of Supervisors with an independent assessment of RCIT's and consolidated departments' compliance with Board Policy A-58, and its applicable standards and internal controls over the safeguarding of network servers. The audit covered the period July 1, 2012, through June 30, 2013.
(Continued on page 2)

Paul Angulo, CPA, CGMA, MA
County Auditor-Controller

Departmental Concurrence

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost:	POLICY/CONSENT (per Exec. Office)
COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0	Consent ☒ Policy ☐
NET COUNTY COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0	

SOURCE OF FUNDS: N/A

Budget Adjustment: No

For Fiscal Year: n/a

C.E.O. RECOMMENDATION: APPROVE

BY: Samuel Wong

County Executive Office Signature Samuel Wong

MINUTES OF THE BOARD OF SUPERVISORS

☐ Positions Added ☐ Change Order

☐ A-30 ☐ 4/5 Vote

Prev. Agn. Ref.: | **District: ALL** | **Agenda Number:** 2-13

BACKGROUND:
Summary (continued)
Based upon the results of our audit, we determined that RCIT's internal controls, especially the control environment, over the Information Security Program did not provide reasonable assurance that county operational and reporting objectives related to assessing, accepting, and mitigating information security risks and compliance with A-58 Policy and standards were met. We determined RCIT's management control over the physical security of network servers provides reasonable assurance that RCIT will achieve its objectives. Reasonable assurance recognizes internal control has limitations, including cost, mistakes, and intentional efforts to bypass internal controls. We will follow-up within one year to determine if actions were taken to correct the findings noted.

Impact on Citizens and Businesses
Provide an assessment of internal controls over the audited areas.

SUPPLEMENTAL:
Additional Fiscal Information
Not applicable

ATTACHMENTS:

A: County of Riverside Auditor-Controller's Office Internal Audit Report 2013-011: Riverside County Information Technology.

Internal Audit Report 2013-011

Riverside County Information Technology

Report Date: November 26, 2014

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Office of Paul Angulo, CPA, CGMA, MA
County of Riverside Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800

www.auditorcontroller.org

COUNTY OF RIVERSIDE
OFFICE OF THE
AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Paul Angulo, CPA, CGMA, MA
AUDITOR-CONTROLLER

November 26, 2014

Christopher Hans
Riverside County Information Technology
3450 14th Street
Riverside, CA 92501

Subject: **Internal Audit Report 2013-011: Riverside County Information Technology**

Dear Mr. Hans:

The Internal Audit Division of the Auditor-Controller's Office has completed an audit of Riverside County Information Technology (RCIT). The audit objective is to provide management and the Board of Supervisors with an independent assessment of RCIT's and consolidated departments' compliance with Board Policy A-58, and its applicable standards and internal controls over the safeguarding of network servers. The audit covered the period July 1, 2012, through June 30, 2013.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and useful information to provide reasonable assurance that our objective as described above is achieved. An internal audit includes the systematic analysis of information to evaluate and improve the effectiveness of internal controls. We believe this audit provides a reasonable basis for our conclusion.

Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Management is responsible for establishing and maintaining adequate internal controls; our responsibility is to assess the adequacy of the internal controls.

Based upon the results of our audit, we determined that RCIT's internal controls, especially the control environment, over the Information Security Program did not provide reasonable assurance that county operational and reporting objectives related to assessing, accepting, and mitigating information security risks and compliance with A-58 Policy and standards were met. We determined RCIT's management control over the physical security of network servers provides reasonable assurance that RCIT will achieve its objectives. Reasonable assurance recognizes internal control has limitation, including cost, mistakes, and intentional efforts to bypass internal controls.

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2013-011: Riverside County Information Technology

We requested, in accordance with paragraph IIC of the Board of Supervisors Resolution 83-338, that management respond to each reported condition and recommendation contained in our report. Management presented their responses orally during two scheduled meetings, however, never provided a written response to be included in the report. We will follow-up in one year to verify that management implemented the corrective actions.

We thank the Riverside County Information Technology management and staff for their cooperation; their assistance contributed significantly to the successful completion of this audit.

Paul Angulo, CPA, CGMA, MA
County Auditor-Controller

Mark W. Cousineau

By: Mark Cousineau, CPA, CIA, CFE
Chief Internal Auditor

Cc: Board of Supervisors
Executive Office
District Attorney
Grand Jury

Table of Contents

Executive Summary

Overview

In an effort to "provide excellent customer service, at a reasonable price, through the dedication and involvement of our team members" Riverside County Information Technology (RCIT) has established six bureaus to address the needs of its customers. The bureaus are Infrastructure & Communications, Business Systems, Departmental Systems, Health & Human Systems, Information Security Office, and Business Administration.

As an Internal Service Fund department, RCIT obtains all of its revenues from services provided to its customers. RCIT reports advances in the areas necessary to continue servicing county departments and other customers throughout Riverside County which includes the following:

- Comprehensive Technology Expertise
- State of the Art Equipment
- Secure Systems
- Streamlining Costs
- Project Management

At the beginning of the review period, July1, 2012 through June 30, 2013, RCIT had a staff of nearly 200. RCIT staff supports information systems, network solutions, web services and enterprise systems. RCIT executive management allocates staff to provide services to customers.

In March of 2012, RCIT was directed by the County of Riverside Executive Office to identify cost saving areas and assess the feasibility of consolidating technology services county-wide. RCIT began the process of consolidation in July of 2012. As of May 2013, seven County departments; Executive Office, Economic Development Agency, Human Resources, Public Defender, Purchasing, Registrar of Voters and Transportation and Land Management Agency had been consolidated. A services agreement is provided to the consolidating department which defines the basic "roles and responsibilities of all parties for support services covered by this agreement, escalation of any support issues, cost details and mechanisms for adding or changing service."

The RCIT executive during our review was Kevin Crawford, who was replaced by Christopher Hans on August 8, 2014. Staffing as of November 30, 2014 was approximately 450.

Audit Objective

Our audit objective is to provide management and the Board of Supervisors with an independent assessment of RCIT's and consolidated IT departments' compliance with Board Policy A-58 and its applicable Standards and adequacy of physical security of network servers.

Audit Conclusion

Based upon the results of our audit, we determined that RCIT's internal controls, especially the control environment, over the Information Security Program did not provide reasonable assurance that county operational and reporting objectives related to assessing, accepting, and mitigating information security risks and compliance with A-58 Policy and Standards were met. We determined RCIT has adequate physical security over network servers.

Table 1 below summarizes the consolidated departments' non-compliance areas we identified:

Table 1: Summary of Consolidated Departments Non-Compliance

Consolidated Departments	Anti-Malware	Event Logging	Vulnerabilities Remediated	Asset Inventory	Highly Available Information	Account Management	Gap Analysis
Agency A	✓	✓	✓	✓	N/A	✓	✓
Agency B	✓	-	✓	✓	✓	✓	✓
Agency C	✓	✓	✓	✓	✓	✓	✓
Agency D	✓	-	✓	✓	-	✓	✓
Agency E	✓	✓	✓	-	N/A	✓	✓
Agency F	-	✓	✓	✓	✓	✓	✓
Agency G	-	-	✓	-	-	✓	✓
Agency H	✓	✓	✓	✓	✓	✓	✓

Legend:

✓	Not in compliance with the Information Security Standard as issued by the Information Security Office.
-	In compliance with the information security standard as issued by the Information Security Office.
N/A	Audit in this area was not applicable to the department systems.

Compliance with A-58 Policy and Standards

Background

On April 7, 2009, the fourth revision to Board of Supervisors Policy A-58, *Information Security Policy (A-58)*, first adopted on July 29, 2003 under agenda item 3.36, was approved under board agenda number 3.33. The revision authorized the Riverside County Chief Information Security Officer (CISCO) to develop and maintain the Riverside County Information Security Program (RCISP) and requires all Riverside County Departments to comply.

The Information Security Program (ISP) is comprised of the Program Framework which establishes the vision, mission and roles & responsibilities for the ISP, the Information Security Risk Management Methodology, the processes for assessing, accepting and mitigating information security risks, and Information Security Standards the specific controls and processes for mitigating information security risks.

Roles and responsibilities have been established to integrate county department's policies and processes, accessibility of systems, archival and destruction of forms. Each department has been assigned a Department Information Security Officer (DISO) who performs the reporting and remediation of any gaps and deficiencies identified once an update occurs with any RCIT issued standards. The RCIT Information Security Office (ISO) assists the DISO "with the implementation and ongoing compliance with the Standard."

The Information Management Standard (IMS) and the Information Security System Standard (ISSS) were included in the audit. The IMS presents two classifications, confidential (C) and highly available (HA) information, which are utilized to "categorize information and define the information security controls" in managing data associated with the respective classification.

Confidential information consists of information which shall not be released under the California Public Records Act, information that by law of public policy may not be disclosed, or if wrongful disclosure could result in moderate or severe business impact.

Highly available information "is that which, if unavailable, would lead to an interruption of County services resulting in a moderate or severe business impact rating."

Objective

Our audit objective is to provide management and the Board of Supervisors with an independent assessment of RCIT's and consolidated departments' compliance with Board Policy A-58 and its applicable standards and physical access controls of servers.

Audit Scope

The scope of this audit included a review of compliance with Board Policy A-58 and its implemented standards: Information Management Standard and Information Security System Standard (A-58 Standards). Detailed testing was performed on RCIT and the following departments who had consolidated with RCIT as of May 2013: Economic Development Agency, Executive Office, Human Resources, Public Defender, Purchasing, Registrar of Voters, and Transportation Land Management Agency.

Audit Methodology

To accomplish our objectives, we:

- Obtained and analyzed Board Policy A-58 and the Information Security Office Standards to gain an understanding of the requirements;
- Conducted interviews with department personnel;
- Compared the A-58 Policy and Information Security Office (ISO) standards issued in March 2009 and subsequent revisions through May 2013;
- Determined if consolidated departments had completed a gap analysis in accordance with information security standards;
- Reviewed the vulnerability scans for selected servers and workstations for a six month period of time;
- Compared actual server and workstation security settings to Information Security Standards using software security tools;
- Reviewed account management policies for compliance with ISSS requirements;
- Reviewed security settings for selected servers and workstations that enable protective software (anti-malware) to function at its highest level.
- Reviewed event logging system and workstation settings and;
- Reviewed asset inventory management.

Results

The Board of Supervisors approved current Board Policy A-58 in April 2009 which includes the standards (e.g. Information Management Standard, Network Standard, and Information Technology Systems Standard). The policy is comprised of the Information Security Program Framework for Riverside County which outlines the vision of the Information Security Program, its mission and the roles & responsibilities for the program. Also, attached to the policy was the Information Security Risk Management Methodology which supports and defines the programs processes for managing risk associated with information security. Further, the methodology identifies in what manner security risks are managed. This process includes mitigating network systems risks within certain timeframes once vulnerability scans of county networks have identified the vulnerabilities.

We identified the minimum requirements for the A-58 Standards revised as of June 12, 2012 and determined that RCIT did fully comply with the security risk methodology identified in the RCISP.

Finding 1: Security Assessments Were Not Performed for Changed Security Standards

RCIT and the seven consolidated IT departments have not performed required security assessments, or gap analyses, that identify the difference between the current system requirements and the new system requirements as required by RCISP. According to department information technology representatives this occurred because they do not have the staff to perform the analysis or they were not aware of the requirement. The policy states specifically, under the Process Activity section of the Information Security Risk Management Methodology, departments must complete gap analysis within 90 days of the release of an Information Security Standard; departments will provide the ISO with monthly status updates; and copies of the completed gap analysis must be provided to the ISO. RCIT's non-enforcement of A-58 policy and the related standards relating to gap analysis could result in a breach in the county's information system.

Recommendation 1.1

RCIT should ensure gap analysis are completed and provided to the Information Security Office as required.

Recommendation 1.2

RCIT should work in conjunction with the ISO to make department staff aware of all RCISP requirements.

Recommendation 1.3

ISO should actively monitor for required gap analysis reports.

Finding 2: Security Vulnerabilities Were Not Promptly Corrected

Results of vulnerabilities identified in the information systems are not remediated within standard response time. We reviewed the vulnerability scans for RCIT and the seven consolidated IT departments for the period February 1, 2013 through June 30, 2013. For each of the departments, five servers and five workstations were selected for testing. In most instances, the risk classifications which ranged from critical to low were not remediated as directed in the standards.

Table 2 below summarizes vulnerability remediation timeframes as detailed in the Information Security Standard:

Table 2: Vulnerability Remediation Timeframes

Risk Classification	Servers, Network Equipment, Storage Systems	Workstations/Mobile Workstations
Critical	48 hours	24 hours
Severe	10 days	5 days
Medium	30 days	15 days
Low	At discretion of DISO*	At discretion of DISO*
DISO – Department Information Security Officer		

Vulnerabilities are reported separately in the vulnerability scanning application for RCIT and the consolidated IT departments. From the scans performed, the departments did not remediate the vulnerabilities identified in the scans within the timeframes specified in the Information Security Standard. Table 3 summarizes the departments' number of vulnerabilities that remained un-remediated for more than a month for the systems we tested:

Table 3: Summary Of Departments Remediation Management Of Vulnerabilities

Department	Critical				Severe				Moderate				Remediated Timely
	AVW	WANM	AVS	SANM	AVW	WANM	AVS	SANM	AVW	WANM	AVS	SANM	
Agency A	141	1.2	245	3.9	5	1.8	12	3.9	38	1.3	84	3.9	No
Agency B	0	0	407	2	4	3	10	2	0	0	201	2	No
Agency C	456	2.9	110	4.6	7	1.9	9	5.4	121	2.7	59	5	No
Agency D	.4	2	3	1.7	3	4.6	9	4.5	0	0	.4	2	No
Agency E	547	4.6	35	3.8	198	4.7	13	4	14	4.9	2	4.2	No
Agency F	45	2.9	6	.7	22	2.8	2	1.4	4	2.6	0	0	No
Agency G	150	3.5	248	4.6	77	3.8	366	4.6	9	4	6.8	4.6	No
Agency H	159	2	147	5	13	3.1	50	5.2	.7	3.7	5.6	4.1	No

Legend:

AVW Average number of vulnerabilities for all workstations tested
WANM Workstation average number of months vulnerabilities remained without being remediated
AVS Average number of vulnerabilities for all servers tested
SANM Server average number of months vulnerabilities remained without being remediated

The causes identified by RCIT and consolidated department IT staff for not timely addressing vulnerabilities were:

1. Do not have the staffing resources to update and patch the systems.
2. Patch management software is not available to update and patch the systems efficiently.
3. Patching the vulnerabilities can be time consuming and competes with other duties.
4. Some vulnerability patches require that it be done in a test environment before being placed in the production environment to identify any potential issues that may arise as a result of the patch.

The A-58 Standards define the minimum requirements for all County information, and the systems, technologies, and processes through which information is created, acquired, processes, stored, transmitted and destroyed. Non-compliance with the minimum requirements as it relates to vulnerability management exposes the County systems and information to potential exploitation and increases the security risk.

Recommendation 2:

RCIT and the ISO should determine an appropriate manner to address vulnerabilities identified in the vulnerability scans within the timeframes allotted in the standards.

Finding 3: Software to Prevent Unauthorized and Harmful Software was Not Used Appropriately

The anti-malware programs meant to protect computers and systems against viruses, spyware and other harmful external programs, are not adequately utilized by the departments. We reviewed the configurations for the anti-virus solutions and found the departments were not in compliance with anti-malware solutions which states the servers and workstations should be configured to weekly full scan, daily updates of scan engine and malware definitions, and sanitation actions set to quarantine and delete. The stated cause per RCIT staff was that they had not been provided the revised A-58 Standards. The standards define the minimum requirements for all County information, and the systems, technologies, and processes through which information is created, acquired, processes, stored, transmitted and destroyed. Not meeting the minimum requirements leave the County systems exposed to malware infiltrations and attacks. Table 4 summarizes the results for each department we reviewed:

Table 4: Summary Of Anti-malware Testing Results

Consolidated Departments	Not set for Full Scan	Not reported Monthly to ISO	Not Quarantined
Agency A	✓	✓	-
Agency B	-	✓	-
Agency C	✓	✓	✓
Agency D	✓	✓	-
Agency E	✓	✓	-
Agency F	-	✓	-
Agency G	-	✓	-
Agency H	✓	✓	✓

Legend:
- \- Compliant with standard
- ✓ Not in compliance

Note: If during our testing, even one of the tested assets did not have the settings in accordance to the standard requirements, our conclusion was non-compliance. The logic is that one infected asset provides an access point for other systems to be infected as intended by antimalware authors.

Recommendation 3.1

Formalize practices for the dissemination of standards and operational changes that includes a requirement for acknowledgment of receipt.

Finding 4: Records of Significant Computer Operations Events Were Not Maintained in Accordance With Standards

The event logs which record significant computer operation events such as user logon and logoffs, update failures and successes; program errors, and other significant events are not properly maintained for 4 of the 8 (or 50%) departments we reviewed during our audit. According to the standards, the logs should be maintained for a minimum of 90 days. Additionally, based on interviews with the RCIT staff and review of event log settings, we found the departments' event logs were not consistent with the standards. For example, the event logs for TLMA indicated log failures but log successes were not found for audit account management, audit policy changes, audit privilege use, restart and shutdown, log on and log off, and user/group management. Also, for Economic Development Agency, the lockout timeframe was set at 30 minutes and the standards state the timeframe should be at 60 minutes. Furthermore, for some of the log settings, log management history was set to be maintained in terms of data size and not in terms of days as indicated above. Discussions revealed that for departments not in compliance, some of the log settings for workstations and servers are left with factory settings and are left unchanged. The Riverside County Information Security Standard states that at minimum, operating systems shall be configured to audit and log system events, security events, network events, and application events. It further states that all logged events shall be retained for a minimum of ninety (90) days. When the event logs are not properly retained or recorded, the ability to identify illegal entries into the county network system could be reduced.

Recommendation 4.1

RCIT should train, test and monitor DISOs on the requirements for event logs and establish a system to confirm compliance.

Recommendation 4.2

RCIT and the ISO determine the memory capacity requirements, whether in terms of data size or in terms of days, that will satisfy the logging requirements detailed in the Information Security Standard.

Finding 5: Accountability of Assets is Difficult to Ascertain

The asset inventory listing of servers and workstations obtained from the consolidated department representatives did not agree with the listing extracted from the Information Security's Office's scanning software. We found assets were listed on the ISO provided list (extracted from their scanning software) but not the departments provided list and vice versa. According to the DISOs in each department, this occurs because when the monthly scans occur, often the systems, which includes servers or workstations, are powered off or are no

longer in service. Furthermore, it was revealed through interviews that IP addresses, which we used to compare the lists, are commonly changed and reassigned to different IT assets. Each department is provided with an IP address range, and all assets connected to the department's network will be assigned an IP address within the range. The ISO's office enters the IP address range in the scanning software for the vulnerability scans. When departments assigned new IP addresses to IT assets outside the range provided to the ISO, the systems outside the range are not scanned for vulnerabilities. Any new ranges need to be forwarded to the ISO timely for entry into the scanning software. Not providing the updates to the ISO, exposes department systems to vulnerabilities.

Recommendation 5.1

RCIT should ensure that any new IP address ranges are submitted to ISO in a timely manner to ensure scan of all IT assets.

Finding 6: User Access to Information Systems were not disabled timely

We identified the following areas for improvement relating to user information account management:

- System account access for terminated or retired information technology staff were not disabled in a timely manner,
- There is no written policy or procedures for disabling account access, and
- Departments could not provide documentation to confirm accounts were deleted.

Further, three out of the eight departments did not disable the account access for terminated employees in a timely manner. In discussions with DISOs, it was stated that this was an oversight. It took 259 days to delete/remove account access for a terminated employee in one of the departments and for another department it took 330 days to disable the account.

For other departments we found the DISO completely deleted the accounts without disabling them. RCIT staff expressed that best practices would be to disable the account prior to deleting the account of the terminated/retired employee. Formal written account management practices are missing, failure to implement account management written procedures results in no accountability over the procedure.

Recommendation 6.1

RCIT should develop account management procedures and utilize it to train all DISO's on the appropriate process for disabling account access.

Recommendation 6.2

Establish an internal control process for disabling account access for terminated/retired employees to ensure compliance with the standard requirements.

Finding 7: Information Security Office Approvals for New Systems Need to be formalized in the Standards Conformance Review

Two of the eight departments did not obtain approval from the Information Security Office prior to implementing new systems into the county network. In both instances, we determined through interviews with IT staff that this occurred because they did not know to submit to the ISO for a conformance review or that the standard required compliance with information security specifications. All new devices should be deployed in compliance with ISO established information security standards and have a conformance review performed by the ISO. It is important to note that even though the A-58 Standards does not specifically require that new systems introduced to the County network have a conformance review performed by the ISO, such practice needs to be standardized by making it a requirement under the A-58 Standards.

Recommendation 7.1

The ISO should formalize the standard by including the requirements in the A-58 Standard if this is the desired practice.

Finding 8: Awareness of BOS policy A-58 and Related Information Security Standards

RCIT staff is not aware of Board of Supervisors Policy A-58 and implemented standards. There were instances internal audit staff was requested to provide copies of the standards being used since staff did not have copies or were not aware of requirements within the standards. It was determined through interviews with staff charged with departmental networks that there is a lack of awareness of Board of Supervisors Policy A-58 Standards. RCIT staff did not know of the policies and standards governing Information Security lead to non-compliance with the minimum requirements for all County information, the systems, technologies, and processes through which information is created, acquired, processed, stored, transmitted, and destroyed. The RCISP is a guide for departments on matters that are not otherwise addressed in state codes, county ordinances and resolutions by the Board of Supervisors. The policy also provides the framework for the Information Security Program. The Information Security Standards define the specific controls and processes required to mitigate information security risks.

Recommendation 8.1

RCIT should implement recurring training of A-58 Standards and ensure ongoing communication to its staff of the importance in complying with the policy and standards.

Business Continuity & Physical Security of Network

Background

Business Continuity is a management process which identifies any risks, threats and vulnerabilities that may impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response. The original plan was completed in 2009 and a revision of the plan is in process. The 2009 document has a disaster recovery plan which requires a Business Continuity Plan (BCP) be completed. The disaster recovery plan is "a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster" and the business continuity plan serves to identify an organizations exposure to internal and external threats. It can be termed as the "roadmap for continuing operations." No date has been set for completion of the BCP.

It was disclosed during September 24, 2013 board meeting that systems are backed up to a secondary location within the county. It is not backed up outside of the county systems but it is backed up to tape which is sent to an offsite location. It does not provide the County with the ability to switch to an alternate system within an hour or two of the system going down. If an event occurs, requiring new hardware, it could take RCIT 5-10 days to get the system running. During the September 24, 2013 board meeting, RCIT stated it had asked the Human Resource and Auditor-Controller departments to keep their information on different systems. RCIT Management is considering swapping data with other northern California counties as an option. Discussions are already underway for this possibility. It was admitted that more needs to be done to improve the disaster recovery plan for Information systems and RCIT has been working towards addressing as many concerns relating to this area as possible.

Audit scope

We reviewed the disaster recovery plan, in lieu of a business continuity plan, to ensure adequate response in the case of an emergency. Additionally, for security of the network assets we confirmed the main network sites and verified the physical controls.

Audit Objective

Our audit objective is to provide management and the Board of Supervisors with an independent assessment of the existence of a business continuity plan and the internal controls over physical security of the county network.

Audit Methodology

To accomplish our objectives, we:

- Obtained an understanding of board policies, applicable standards and best business practices related to physical security of IT assets;
- Conducted interviews with department personnel and the Information Security Office staff;
- Observed the physical locations of the network sites and;

- Reviewed the most recent Disaster Recovery Plan.

Results

RCIT has multiple locations throughout the county. As such, they have segregated the servers to better assist in the daily operations of departments. During the audit, we randomly selected locations to observe the network servers were away from hazardous operations, in a clean and stable environment and contained fire detection devices as well as fire extinguishers. Further we determined if the network server room was restricted to authorized personnel. Based on our review of guidelines, interviews with RCIT personnel and observations of their facilities, we determined the physical security was adequate.

Since RCIT never completed the current business continuity plan we reviewed the department's disaster recovery plan of 2009 which RCIT staff state is the most recent. This plan is not current and does not address some of the best business practices areas:

- Weekly data back-ups are performed and media stored off site;
- Off-site location storage adequate in comparison with industry best practices;
- Uninterrupted Power Supply equipment identified, made available and installed;
- Annual testing of the plan;
- Detailed arrangements for immediate replacement of essential hardware;
- Written process for restoration of backed up data.

Finding 9: Disaster Recovery

RCIT stated they utilize their disaster recovery plan which does not focus on best practices for business continuity plan areas such as weekly data back-ups, restoring from back-up status, annual testing of the plan, detailed arrangements for immediate replacement of essential hardware, and written processes for restoration of backed up data. With a new Chief Information Officer at the helm, the department has been in the process of revising the disaster recovery plan to address the areas identified for a business continuity plan. Without an actionable plan in place the county may be exposed to internal and external risk.

Recommendation 9.1

RCIT should complete a business continuity plan and submit to the Board for approval as early as possible.