Internal Audit Department

ORANGE COUNTY
6th Largest County in the USA

INFORMATION TECHNOLOGY AUDIT:
SHERIFF-CORONER COMPUTER GENERAL CONTROLS

As of September 30, 2014

We audited select computer general controls over the administration and use of Sheriff-Coroner's (S-C) computing resources by reviewing applicable policies and procedures and conducting interviews with IT management.

Based on the work performed, IT general controls were found adequate, including:

1) **Adequate security-related policies and procedures have been developed including security awareness and other security-related personnel policies;**
2) **Adequate user access and physical access general controls policies and procedures were present to provide reasonable assurance that computer resources are protected from unauthorized personnel;**
3) **Adequate configuration management policies and procedures, including change management, have been developed;**
4) **Adequate segregation of duties exists within the IT function;**
5) **Adequate policies and procedures for disaster recovery/business continuity have been developed to help mitigate service interruptions.**

Our audit identified four (4) Control Findings for security settings, change management policies and procedures, computer operations policies and procedures, and contingency planning.

AUDIT NO: 1353
REPORT DATE: JANUARY 13, 2015

Director: Dr. Peter Hughes, MBA, CPA, CITP
Assistant Director/Senior Audit Manager: Michael Goodwin, CPA, CIA
IT Audit Manager: Wilson Crider, CPA, CISA*

(*Certified Information Systems Auditor)

Independence • Objectivity • Integrity

ORANGE COUNTY BOARD OF SUPERVISORS'
OC Internal Audit Department

GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010, 2013

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes **Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF, CGMA**
Director
Certified Compliance & Ethics Professional (CCEP)
Certified Information Technology Professional (CITP)
Certified Internal Auditor (CIA)
Certified Fraud Examiner (CFE)
Certified in Financial Forensics (CFF)
Chartered Global Management Accountant (CGMA)
E-mail: peter.hughes@iad.ocgov.com

Michael Goodwin **CPA, CIA**
Assistant Director/
Senior Audit Manager

Alan Marcum **MBA, CPA, CIA, CFE**
Senior Audit Manager

Autumn McKinney **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Information Systems Auditor (CISA)
Certified Financial Government Manager (CGFM)

Hall of Finance & Records

12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit

OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 1353 January 13, 2015

TO: Sandra Hutchens
Sheriff-Coroner

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Information Technology Audit:
Sheriff-Coroner Computer General Controls

We have completed an Information Technology Audit of Sheriff-Coroner - Computer General Controls as of September 30, 2014. We performed this audit in accordance with our *FY 2013-14 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. Our final report is attached for your review.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). Our **first Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **second Follow-Up Audit** will begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented. At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

Each month I submit an **Audit Status Report** to the BOS where I detail any critical and significant audit findings released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this audit will be included in a future status report to the BOS.

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report. Additionally, we will request your department complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

Attachments

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 5.

OC Internal Auditor's Report

Information Technology Audit:
Sheriff-Coroner
Computer General Controls
Audit No. 1353

As of September 30, 2014

OC Internal Auditor's Report

Audit No. 1353 **January 13, 2015**

TO: Sandra Hutchens
Sheriff-Coroner

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Information Technology Audit: Sheriff-Coroner Computer General Controls

Audit Highlight

The Orange County Sheriff-Coroner Department is a large, multi-faceted law enforcement agency served by approximately 4,000 sworn and professional staff members and over 800 reserve personnel. The Sheriff delegates authority to her executive team made up of one Undersheriff, three Assistant Sheriffs, an Executive Director, three Commanders and one Senior Director, who administers the daily activities of the captains and professional staff at the division head level.

Sheriff-Coroner (S-C) Information Technology is managed by an IT Manager, who reports to the Support Services Director. The S-C Information Technology department consists of approximately fifty (50) staff.

We identified **four (4) Control Findings** relating to security settings, change management policies and procedures, computer operations policies and procedures, and contingency planning.

OBJECTIVES

In accordance with our *FY 2013-2014 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors, we conducted an Information Technology Audit of Sheriff-Coroner (S-C) - Computer General Controls. This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236. The objectives of our audit were to:

1. Evaluate the adequacy of S-C's security-related policies and procedures including security awareness and security-related personnel policies;
2. Evaluate the adequacy of user access and physical access general controls policies and procedures to provide reasonable assurance that computer resources are protected from unauthorized personnel;
3. Evaluate the adequacy of S-C's configuration management policies and procedures to help ensure only authorized programs and authorized modifications are implemented and errors are not introduced into programs when they are developed or subsequently modified;
4. Evaluate whether segregation of duties exists within the IT function; and
5. Evaluate the adequacy of S-C's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions.

RESULTS

Objective #1: Our audit found **adequate** security-related policies and procedures including security awareness and other security-related personnel policies. No findings were identified under this objective.

Objective #2: Our audit found **adequate** policies and procedures for user access and physical access general controls that provide reasonable assurance computer resources are protected from unauthorized personnel. We identified **one (1) Control Finding** regarding security settings.

Objective #3: Our audit found **adequate** configuration management policies and procedures. We identified **two (2) Control Findings** for improving change control and computer operation policies and procedures.

Objective #4: Our audit found **adequate** segregation of duties exists in the IT function. No findings were identified under this objective.

Objective #5: Our audit found that **adequate** policies and procedures for disaster recovery/business continuity have been developed to help mitigate service interruptions. We identified **one (1) Control Finding** regarding contingency planning.

The following table summarizes our findings and recommendations for this audit. See further discussion in the *Detailed Results, Findings, Recommendations and Management Responses* section of this report. See *Attachment A* for a description of Report Item Classifications.

Summary Table of Findings and Recommendations

Finding No.	Finding Classification (see Attachment A)	Finding and Page No. in Audit Report	Recommendation	Concurrence by Management?
1.	**Control Finding**	S-C security settings may be improved (p.7).	S-C should change the network security settings to meet best practices.	Yes
2.	**Control Finding**	S-C has draft change management policies and procedures that do not address vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, or patch management (p.8).	S-C should develop policies and procedures to address: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management.	Yes
3.	**Control Finding**	Computer operation policies and procedures were not documented (p.9).	S-C should document and maintain its computer operation policies and procedures.	Yes
4.	**Control Finding**	The S-C disaster recovery and contingency plans have not been updated or tested within the past year (p.11).	S-C should develop a plan for testing its disaster recovery and contingency plans on a regular basis.	Yes

BACKGROUND

The Sheriff-Coroner Department is a large, multi-faceted law enforcement agency served by approximately 4,000 sworn and professional staff members and over 800 reserve personnel. The Sheriff oversees an executive team made up of an Undersheriff, three Assistant Sheriffs, an Executive Director, three Commanders and a Senior Director. The department consists of five organizational Commands comprised of 21 separate Divisions:

- **Executive Command** – includes Sheriff's Executive Management, Community Services and Media/Government Relations.
- **Administrative Services Command** – includes Communications, Financial/Administrative Services, Research & Development and Support Services.
- **Custody Operations and Court Services Command** – includes the three Jail Facilities, Inmate Services and Court Operations.
- **Field Operations & Investigative Services Command** – includes Airport Operations, Homeland Security, North and South Patrol Operations and Investigations.
- **Professional Services Command** – includes Coroner Services, Crime Lab, Professional Standards, S.A.F.E., and Training.

Information Systems Bureau

S-C Information Systems Bureau is managed by an IT Manager, who reports to the Support Services Director. The S-C Information Systems Bureau consists of approximately fifty (50) staff organized into the following areas: Field Base Reporting (FBR) Project Manager, IT Project Manager Enterprise Applications, Infrastructure, and IT Project Manager CRM Applications. S-C utilizes a number of critical systems in their day-to-day law enforcement operations including:

- Sheriff's Data System (SDS)/Automated Jail System (AJS),
- Enhanced Law Enforcement Telecommunications Emulator (ELETE),
- BMC Remedy AR Systems (Help Desk/Asset Inventory Reporting),
- Records Management System (RMS), and
- Computer Aided Dispatch (CAD) backup.

These systems store and process sensitive/confidential data including law enforcement operations involving criminal investigations, jail operations, undercover and forensic work. In addition, these systems interface with other key statewide and Department of Justice law enforcement systems. Therefore, restricting access to the systems and their data is a key priority.

Definition of Computer General Controls: General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. For this reason, general controls are usually evaluated separately from and prior to evaluating application controls. This audit focuses only on computer general controls.

Definition of Application Controls: Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer, and are generally categorized into three phases:

- **Input:** Data is authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner;
- **Processing:** Data is properly processed by the computer and files are updated correctly; and
- **Output:** Files and reports generated by the application actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

Definition Source: Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM).

SCOPE AND METHODOLOGY

Our audit evaluated policies and procedures over select general controls (see definition above) over the administration and use of S-C's computing resources as of September 30, 2014. Our methodology included inquiry, auditor observation, and limited testing of policies and procedures over the following:

1. The adequacy of S-C's security-related policies and procedures including security awareness and other security-related personnel policies. We examined security-related personnel policies that are critical to effective security such as screening and training employees, and monitoring the effectiveness of the security program.

2. The adequacy of general user access and physical access controls over computer resources to provide reasonable assurance that computer resources are protected from unauthorized personnel. We examined access control-related policies and procedures and performed limited testing to ensure the access controls are effective, properly authorized, implemented and maintained.

3. The adequacy of S-C's configuration management policies and procedures to help ensure only authorized programs and authorized modifications are implemented and errors are not introduced into programs when they are developed or subsequently modified.

4. The adequacy of segregation of duties within the IT function. We evaluated the roles and responsibilities of S-C Information Technology to ensure no one individual has incompatible IT duties that could bypass established general computer controls.

5. The adequacy of general controls, primarily S-C's policies and procedures, over disaster recovery/business continuity to help mitigate service interruptions. We assessed the level of completion in the Countywide business continuity plan program and examined related disaster recovery/business continuity documentation.

To accomplish our scope, we obtained an understanding of selected S-C general controls and compared them with the Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM) identified control objectives.

SCOPE EXCLUSIONS

Our audit did not include an audit or review of the following:

1. Application controls. This audit included only computer general controls (see above definition).
2. Security settings for operating system, file directory, database, and remote access (telecommunication) other than reviewing policy and procedures for their appropriate configuration.
3. Compliance with laws and regulations including DMV security agreement and FBI Criminal Justice Information Services.
4. Controls or processes performed by other parties including CEO/IT data center physical controls, network monitoring, intrusion/detection, firewall, remote access, etc.
5. Security management controls provided at the County level including establishing an entity-wide security management program, periodically assessing and validating risks, and monitoring the effectiveness of the County security program.
6. Access control objectives provided at the County level including adequately protecting information system boundaries, resources, and implementing effective audit and monitoring capabilities.
7. Configuration management controls including maintaining current configuration identification information and routinely monitoring configurations.
8. Contingency planning control objectives managed at the County level including developing and documenting a comprehensive contingency plan and periodically testing the contingency plan and adjusting it as appropriate.
9. We did not assess all control techniques or perform all potential audit procedures identified in FISCAM. Internal Audit made a determination of which general controls were included in the audit.

Management's Responsibilities for Internal Controls

In accordance with the Auditor-Controller's County Accounting Manual Section S-2 *Internal Control Systems*: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Control systems shall be continuously evaluated by Management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating an entity's internal control structure is the Committee of Sponsoring Organizations (COSO) control framework. Our Internal Control Audit enhances and complements, but does not substitute for the Sheriff-Coroner's continuing emphasis on control activities and self-assessment of control risks.

Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the Sheriff-Coroner's operating procedures, accounting practices, and compliance with County policy.

Acknowledgment

We appreciate the courtesy extended to us by Sheriff-Coroner's personnel during our audit. If we can be of further assistance, please contact me directly at 834-5475 or Michael Goodwin, Assistant Director at 834-6066.

Attachments

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Don Barnes, Assistant Sheriff, Administrative Services Command, S-C
Brian Wayt, Senior Director, Administrative Services Command, S-C
Kirk Wilkerson, Director, Support Services, S-C
Ed Lee, Administrative Manager, Information Systems Bureau, S-C
Jerry Soto, Administrative Manager, Information Systems Bureau, S-C
Charles Ko, Database & Security Administrator, Information Systems Bureau, S-C
Noma Crook-Williams, Director, Financial/Administrative Services, S-C
Nasrin Soliman, Audit Manager, S-C
Foreperson, Grand Jury
Susan Novak, Clerk of the Board of Supervisors
Macias, Gini & O'Connell LLP, County External Auditor

Objective #1: Evaluate the adequacy of S-C's security-related policies and procedures including security awareness and other security-related personnel policies.

Work Performed

To accomplish this objective, we obtained and reviewed S-C's security-related policies and procedures including security awareness and other security-related policies. Specifically, we interviewed S-C IT staff; reviewed S-C security-related policies and procedures including County IT Security Policy, County IT Usage Policy, OC Sheriff Department (OCSD) IT Policy, OCSD Electronic Communications Policy, OCSD Policy Manual, OCSD Equipment Issue Inventory, and other S-C policies and procedures. In addition, we obtained a security vulnerability assessment performed by Foundstone, a division of McAfee that provides external security assessments, and reviewed the identification of security weaknesses and remediation of the issues.

Our evaluation of the policies and procedures noted that:

- Adequate security control policies and procedures are documented and address:
  - Security risk assessment;
  - Purpose, scope, roles, responsibilities, and compliance;
  - Users will be held accountable for their actions;
  - S-C is subject to both *County IT Usage and IT Security Policy* requirements; and
  - S-C provided security awareness training on Information Security and Privacy.
- Adequate security awareness and other security-related personnel policies are documented and address:
  - Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors;
  - Hiring, transfer, termination, and performance policies address security;
  - Non-disclosure or security access agreements are required for employees and contractors assigned to work with sensitive information;
  - Formal sanctions process is employed for personnel failing to comply with security policy and procedures;
  - Termination and transfer procedures include: exit interviews procedures; return of property, keys, identification cards, passes, etc.; and notification to security management of terminations and prompt revocation of IDs and passwords; and
  - Employee training and professional development is provided and available to S-C staff.
- Foundstone, a division of McAfee that provides external security assessments, conducted a vulnerability assessment of the S-C computing environment. We reviewed the report and noted identified issues were resolved by S-C.

Conclusion

Based on the work performed, adequate security-related policies and procedures have been developed including security awareness and other security-related personnel policies. Our audit found that S-C partnered effectively with County Executive Office/Information Technology in establishing, maintaining, and monitoring security of computer general controls.

As such, we have no findings and recommendations under this audit objective.

Objective #2: Evaluate the adequacy of user access and physical access general controls to provide reasonable assurance that computer resources are protected from unauthorized personnel.

Work Performed
We audited general computer controls and processes over access to the S-C's computing resources located in Santa Ana. We reviewed system security settings for the S-C network. We discussed network system procedures with S-C IT Staff. We visited the room housing S-C's computing resources and observed selected controls for restricting access to S-C computing resources. We selected a sample of user access to verify access was authorized, and a sample of users to verify their access was removed in a timely manner. Our evaluation of controls and processes noted that:

- S-C implemented adequate identification and authentication mechanisms, including network system security settings for accessing S-C's computing resources that were appropriate and complied with best practices including minimum password length and password complexity.
- S-C implemented adequate authorization controls.
- Physical controls for restricting access to S-C's computing resources located in Santa Ana were adequate and included:
  - Computers reside in locked or otherwise restricted areas;
  - Combinations, keys, or magnetic card keys are given to authorized personnel;
  - Issuance of combinations, keys, or magnetic cards keys is documented and controlled; and
  - Workstations are logically locked when not in use.
- Access to S-C's network was authorized and adequately documented.
- Access to S-C's network for separated employees was removed per the S-C policy.

Conclusion
Based on the work performed, adequate user access and physical access general controls were present to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards. However, our audit disclosed one issue that impacts access to S-C's computing resources. We identified **one (1) Control Finding** to improve and enhance controls and processes in addressing security settings. The finding and recommendation is discussed below.

Finding No. 1 – Security Settings May Be Improved (Control Finding)

Summary
S-C security settings could be enhanced based on various industry standards. S-C configured the settings to allow users to access the system with minimal assistance from S-C Information Systems personnel due to limited resources available to effectively process a high volume of user requests for access and support. The current security settings increase the risk of an unauthorized access to the OCSD network.

Details
Because of the sensitivity of the issues and risks of disclosing specific details, we have not detailed the specifics in this report. The details of the finding were provided to selected personnel within S-C/Information Systems Bureau.

Recommendation No.1
Sheriff-Coroner should consider changing the security settings to meet best practices.

Sheriff-Coroner Management Response:
Concur. Sheriff-Coroner will implement the new security settings to meet best security practices within the next 12 months.

Objective #3: Evaluate the adequacy of S-C's configuration management policies and procedures to help ensure only authorized programs and authorized modifications are implemented and errors are not introduced into programs when they are developed or subsequently modified.

Work Performed
To accomplish this objective, we reviewed policies and procedures over configuration management. We reviewed written procedures for implementing new systems and modifications to systems from request to installation. Our evaluation of policies and procedures noted that:

- Configuration management policies and procedures have been developed and address:
  - Roles, responsibilities, procedures, and documentation requirements.
  - Review and approval of changes by management.
  - System Development Life Cycle methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system; and
  - Appropriate system documentation.
- Configuration changes are properly authorized, tested, approved, tracked, and controlled.

Conclusion
Based on the work performed, adequate system development and change control policies and procedures had been developed to help ensure only authorized programs and authorized modifications are implemented and that errors are not introduced into programs when they are developed or as a result of subsequent modifications. However, our audit disclosed one issue that impacts systems development and change control policies and procedures. We identified **two (2) Control Findings** to improve and enhance controls and processes in addressing change control and computer operations policies and procedures. The findings and recommendations are discussed below.

Finding No. 2 – Change Control Policies and Procedures Need to be Developed (Control Finding)

Summary
Policies and procedures need to address the following: **vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management** to ensure an effective security environment.

Details
Current S-C policies and procedures do not address: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management. Although policies are not critical to the organization, having effective policies in place can reduce the risk of duplicate efforts and incompatibilities between various computer installations. S-C is in the process of updating its policies and procedures. Without effective policies, specific security procedures implemented by OCSD may be less than adequate.

Recommendation No.2
Sheriff-Coroner should develop policies and procedures to address: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management.

Sheriff-Coroner Management Response:
Concur. New policies and procedures in these recommended areas will be developed and become part of the new computer operation policies and procedures established in recommendation #3 within the next twelve months (Also see the response in recommendation #3).

Finding No. 3 – Computer Operations Policies and Procedures Need to be Developed (Control Finding)

Summary
Because the S-C has limited resources available to document and maintain its operations procedures, the computer operation policies and procedures have not been documented. Although policies and procedures are not critical to the organization, having effective policies and procedures in place can reduce the risk of duplicate efforts and incompatibilities between various computer installations.

Details
During our audit, we were informed that S-C was in the process of documenting its computer operation policies and procedures. Effective policies and procedures would address the following aspects of the computer operations: Administrative Procedures (absence notification, building access, change control, data center requests, incident response, requisitioning services and supplies, etc.), Application Development & Support (development practices, development environment, configuration management, system life cycle, required documentation, etc.), Desktop Services (network maintenance and support, software deployment, help desk procedures, remote access, etc.), Network Services (domain administration, disaster recovery, network monitoring, account requests and support, etc.), Project Management, and Training and Standards.

Recommendation No.3
Sheriff-Coroner should document and maintain its computer operation policies and procedures.

Sheriff-Coroner Management Response
Concur. New computer operations policies and procedures will be developed within the next 12 months. These policies and procedures will be maintained and updated.

Objective #4: Evaluate whether segregation of duties exists within the IT function.

Work Performed
To accomplish this objective, we reviewed S-C's IT organization chart and job descriptions for the approximately fifty (50) staff working in the IT function. We evaluated IT staff duties to determine if incompatible duties exist in the areas of IT Management, Application Programming, Systems Programming, Library Management, Production Control, Data Security, and Database and Network administration. Due to S-C's having a client/server platform environment, roles typically associated with a mainframe environment are not necessary such as librarian, computer operator, production control, or data control personnel. In addition, commercial off-the-shelf applications are utilized; accordingly, no personnel are needed or assigned as System Programmers. No incompatible IT duties were noted in our audit.

Conclusion
Based on the work performed, an adequate segregation of duties exists in the IT function.

As such, we have no findings and recommendations under this audit objective.

Objective #5: Evaluate the adequacy of S-C's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions.

Work Performed

To accomplish this objective, we reviewed applicable policies and procedures for backup and recovery. We also determined whether S-C was participating in the CEO/IT contingency planning project and the status of their involvement. We observed controls to protect computing resources from environmental hazards at the rooms housing S-C's computing resources in Santa Ana. Our evaluation of controls and processes noted that:

- Written backup and recovery procedures were appropriate and addressed the following:
  - Backups (system, data, full, incremental) are taken regularly;
  - The backup scheme allows the system to be restored to within 24 hours of the incident;
  - On-site backup tapes are stored in secured, locked and fireproof facilities;
  - Off-site backup tapes are stored in secured, locked and fireproof facilities;
  - Backup tapes are rotated between on-site and off-site storage facilities; and
  - Recovery procedures are documented.

- S-C was participating in the CEO/IT contingency planning project and is **100% complete** with Phase One as of September 30, 2014.

- Controls to protect computing resources from environmental hazards at the room housing S-C's computing resources in Santa Ana were adequate and included:
  - Access to the building is restricted to S-C employees. Visitors may access via the main entrance controlled by Sheriff Deputy. Elevators require access card;
  - Computer room is restricted to IT staff via fingerprint reader;
  - Computer room has separate AC system with building as backup;
  - Computer room has emergency power shut off;
  - Smoke detection devices are installed to provide early warning;
  - Automated fire extinguishing systems are installed;
  - Data center sensors are tied to building panel monitored by central facility;
  - A camera is installed in the computer room;
  - Hand held fire extinguishers are located in strategic locations near the computer;
  - Raised flooring;
  - Computers are secured in rack mounts and bolted to the floor;
  - Uninterrupted power supply (UPS) units are installed for all significant system components;
  - Computer room is supported by a diesel backup generator; tested monthly by OCPW;
  - Emergency lighting has been installed; and
  - Protection systems are maintained regularly.

Conclusion

Based on the work performed, adequate policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions. However, our audit disclosed one issue that impacts access to S-C's computing resources. We identified **one (1) Control Finding** to improve and enhance controls and processes regarding contingency planning. The finding and recommendation is discussed below.

Finding No. 4 – Contingency Plans Need to Be Updated and Tested (Control Finding)

Summary
S-C has not updated or tested IT related contingency plans within the last year. Developing, implementing, testing, and maintaining both a disaster recovery plan and a business contingency plan can save time and money should a disaster occur.

Details
Due to S-C's limited available resources, its contingency plans have not been updated or tested within the last year. Disaster recovery plans provide step by step instructions to resume information systems operations while business contingency plans provide step by step instructions for resuming critical business applications. Without these plans, valuable time may be lost and excessive amounts may be spent to restore business operations. Having current plans that are properly tested ensure that staff are familiar with the procedures and identifies issues that were not anticipated when developed. These issues may then be addressed prior to using the plans during an actual event.

Recommendation No.4
Sheriff-Coroner should develop a plan for testing its disaster recovery and contingency plans on a regular basis.

Sheriff-Coroner Management Response:
Concur. Sheriff-Coroner is currently implementing an IT disaster recovery project which is anticipated to be completed in 24 months. Part of the scope of this project is to work with County's Business Continuity Working Group (BCWG) to regularly update and test the disaster recovery and contingency plan.

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we will classify audit report items into three distinct categories:

- **Critical Control Weaknesses:**
  Audit findings or a combination of Significant Control Weaknesses that represent serious exceptions to the audit objective(s), policy and/or business goals. Management is expected to address Critical Control Weaknesses brought to their attention immediately.

- **Significant Control Weaknesses:**
  Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of internal controls. Significant Control Weaknesses require prompt corrective actions.

- **Control Findings:**
  Audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: Sheriff-Coroner Management Responses

ORANGE COUNTY SHERIFF'S DEPARTMENT
EXTERNAL MEMO

TO: Dr. Peter Hughes, CPA, Director
Orange County Internal Audit Department

FROM: Senior Director Brian Wayt
Administrative Services Command

DATE: December 31, 2014

RE: OCSD Information Technology Audit Responses on Confidential Draft Report No. 1353

Per your request, attached are our responses to the recommendations for the Sheriff-Coroner Information Technology Audit Draft Report No. 1353.

If you have any questions, please contact Nasrin Soliman, Audit Manager of my staff at (714) 834-3201 or me at (714) 647-1803 for further assistance.

c: Undersheriff John Scott, Orange County Sheriff Department
Assistant Sherriff Don Barnes, Orange County Sheriff Department
Director Noma M. Crook, Financial/Administrative Services Division
Director Kirk Wilkerson, Support Services Division
Sharon Tabata, Assistant Director, Financial/Administrative Services Division
Ed Lee, Administrative Manager II, Support Services Division
Linh Vuong, Cost/Audit Manager, Financial/Administrative Services Division
Nasrin Soliman, Audit Manager, Financial/Administrative Services Division
Michael Goodwin, Assistant Director, Orange County Internal Audit

Page 1 of 1

ATTACHMENT B: Sheriff-Coroner Management Responses (continued)

Sheriff-Controller Department
Information Technology Audit
Computer General Controls
Responses for Draft Report, Audit No. 1353

Finding No. 1 – Security Settings may be improved (Control Finding).

Summary:

Sheriff-Coroner (S-C) security settings could be enhanced based on various industry standards. S-C configured the settings to allow users to access the system with minimal assistance from S-C Information Systems personnel due to limited resources available to effectively process a high volume of user requests for access and support. The current security settings increase the risk of an unauthorized access to the OCSD network.

Recommendation No. 1:

S-C should consider changing the security settings to meet best practices.

View of Responsible Official and Planned Corrective Action:

Concur, Sheriff-Coroner will implement the new security settings to meet best security practices within the next 12 months.

Finding No. 2 – Change control policies and procedures need to be developed (Control Finding).

Summary:

Policies and procedures need to address the following: vendor supplied passwords, embedded passwords, development environment, change to network devices, personal and public domain software, and patch management to ensure an effective security environment.

Recommendation No. 2:

S-C should develop policies and procedures to address: vendor supplied passwords, embedded passwords, development environment, changes to network devises, personal and public domain software, and patch management.

View of Responsible Official and Planned Corrective Action:

Concur, new policies and procedures in these recommended areas will be developed and become part of the new computer operation policies and procedures established in recommendation #3 within the next 12 months (Also see the response in recommendation #3).

Finding No. 3 – Computer operations policies and procedures need to be developed (Control Finding).

Summary:

Because the S-C has limited resources available to document and maintain its operations procedures, the computer operation policies and procedures have not been documented. Although policies and procedures are not critical to the organization, having effective policies and procedures in place can reduce the risk of duplicate efforts and incompatibilities between various computer installations.

ATTACHMENT B: Sheriff-Coroner Management Responses (continued)

Sheriff-Controller Department
Information Technology Audit
Computer General Controls
Responses for Draft Report, Audit No. 1353
Page 2

Recommendation No. 3:

S-C should document and maintain its computer operation policies and procedures.

View of Responsible Official and Planned Corrective Action:

Concur, new computer operation policies and procedures will be developed within the next 12 months. These policies and procedures will be maintained and updated.

Finding No. 4 – Contingency plans need to be updated and tested (Control Finding).

Summary:

S-C has not updated or tested IT related contingency plans within the last year. Developing, implementing, testing, and maintaining both a disaster recovery plan and a business contingency plan can save time and money should a disaster occur.

Recommendation No. 4:

S-C should develop a plan for testing its disaster recovery and contingency plans on a regular basis.

View of Responsible Official and Planned Corrective Action:

Concur, Sheriff-Coroner is currently implementing an IT disaster recovery project which is anticipated to be completed in 24 months. Part of the scope of this project is to work with County's Business Continuity Working Group (BCWG) to regularly update and test the disaster recovery and contingency plan.