

# Internal Audit Department

O R A N G E C O U N T Y  
6<sup>th</sup> Largest County in the USA

## INFORMATION TECHNOLOGY AUDIT:

### Key Control Audit

## DISTRICT ATTORNEY COMPUTER GENERAL CONTROLS

As of May 31, 2012

We audited selected computer general controls over the administration and use of the District Attorney's (DA) computing resources by reviewing applicable policies and procedures and conducting interviews with IT management.

Based on the audit, **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 and information security weaknesses have been effectively remediated;
- 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; and
- 5) Adequate policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions and protect computing resources from environmental hazards.

Our audit identified **one (1) Control Finding** regarding business continuity plan documentation.

AUDIT NO: 1143

REPORT DATE: APRIL 29, 2013

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

**RISK BASED AUDITING**

GAO & IIA Peer Review Compliant – 2001, 2004, 2007, 2010



American Institute of Certified Public Accountants Award to Dr. Peter Hughes as 2010 Outstanding CPA of the Year for Local Government

GRC (Government, Risk & Compliance) Group 2010 Award to IAD as MVP in Risk Management



2009 Association of Certified Fraud Examiners' Hubbard Award to Dr. Peter Hughes for the Most Outstanding Article of the Year – Ethics Pays



2008 Association of Local Government Auditors' Bronze Website Award



2005 Institute of Internal Auditors' Award for Recognition of Commitment to Professional Excellence, Quality, and Outreach

 ORANGE COUNTY BOARD OF SUPERVISORS'  
**Internal Audit Department**

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

*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

---

**Eli Littner** **CPA, CIA, CFE, CFS, CISA**  
Deputy Director Certified Fraud Specialist (CFS)  
Certified Information Systems Auditor (CISA)

**Michael Goodwin** **CPA, CIA**  
Senior Audit Manager

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

**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](http://www.ocgov.com/audit)



**OC Fraud Hotline (714) 834-3608**



## Transmittal Letter



**Audit No. 1143**    **April 29, 2013**

**TO:** Tony Rackauckas  
District Attorney

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

**SUBJECT:** Information Technology Audit:  
District Attorney  
Computer General Controls

We have completed an Information Technology Audit of the District Attorney - Computer General Controls as of May 31, 2012. We performed this audit in accordance with our *FY 2011-12 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.

We have attached a **Follow-Up Audit Report Form**. Your agency should complete this template as our audit recommendations are implemented. When we perform our first Follow-Up Audit six months from the date of this report, we will need to obtain the completed document to facilitate our review.

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 or recommendation. 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 4.

# Table of Contents



*Information Technology Audit:  
District Attorney  
Computer General Controls  
Audit No. 1143*

As of May 31, 2012

|  |           |
|--|-----------|
| <b>Transmittal Letter</b>  | <b>i</b>  |
| <b>OC Internal Auditor's Report</b>  |           |
| <b>OBJECTIVES</b>  | <b>1</b>  |
| <b>RESULTS</b>   | <b>1</b>  |
| <b>BACKGROUND</b>  | <b>2</b>  |
| <b>SCOPE AND METHODOLOGY</b>   | <b>3</b>  |
| <b>SCOPE EXCLUSIONS</b>  | <b>4</b>  |
| <b>Detailed Results, Findings, Recommendations and Management Responses</b>                          |           |
| <b>Finding No. 1 – Need to Complete Business Continuity Planning Documents<br/>(Control Finding)</b> | <b>9</b>  |
| <b>ATTACHMENT A: Report Item Classifications</b>   | <b>11</b> |
| <b>ATTACHMENT B: District Attorney Management Response</b>   | <b>12</b> |



**Audit No. 1143**

**April 29, 2013**

TO: Tony Rackauckas  
District Attorney

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

A handwritten signature in blue ink that reads "Peter Hughes".

SUBJECT: Information Technology Audit: District Attorney  
Computer General Controls

## Audit Highlight

The Office of the District Attorney represents the People of California in some civil and in most criminal proceedings. Headed by the District Attorney, the Office has a budget of \$114 million and a staff of 723 including executive managers, attorneys, investigative staff, paralegals and legal support staff, and administrative staff. The Office's 250 attorneys annually prosecute over 80,000 cases.

Our audit found that: 1) adequate security-related policies and procedures have been developed; 2) adequate user access and physical access general controls were present; 3) adequate configuration management policies and procedures have been developed; 4) adequate segregation of duties exists within the IT function; and 5) adequate policies and procedures for disaster recovery/business continuity have been substantially developed and protect computing resources from environmental hazards. We identified **one (1) Control Finding** regarding business continuity plan documents.

## OBJECTIVES

In accordance with our *FY 2011-2012 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors, we conducted an Information Technology Audit of the District Attorney - **Computer General Controls**. Our audit was conducted in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. The objectives of our audit were to:

1. Evaluate the adequacy of DA's security-related policies and procedures including security awareness and security-related personnel policies and information security weaknesses are effectively remediated;
2. Evaluate the adequacy of user access and physical access general control policies and procedures to provide reasonable assurance that computer resources are protected from unauthorized personnel;
3. Evaluate the adequacy of DA'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 DA's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions and protect computing resources from environmental hazards.

## RESULTS

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

**Objective #3:** Our audit found **adequate** configuration management policies and procedures. No findings were identified under this objective.

**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 had been substantially developed to help mitigate service interruptions and protect computing resources from environmental hazards. We identified **one (1) Control Finding** regarding further development of business continuity plan documents.

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

| Finding No. | Finding Classification | Finding   | Recommendation   | Concurrence by Management? | Page No. in Audit Report |
|-------------|------------------------|---|--|----------------------------|--------------------------|
| 1.          | <b>Control Finding</b> | <u>Need to Complete Business Continuity Planning Documents</u> - DA has completed and submitted about 18% of the Business Continuity Plan documents (Phase 1 of 2) to CEO/IT. | DA should make completion of the County's Business Continuity Plan documents a priority. | Yes                        | 9-10                     |

## BACKGROUND

The Office of the District Attorney represents the People of California in some civil and in most criminal proceedings. Headed by the District Attorney, the Office has a budget of \$114 million and a staff of 723 including executive managers, attorneys, investigative staff, paralegals and legal support staff, and administrative staff. DA personnel are located in five Justice Centers (Central, Harbor, North, West, and Juvenile) throughout the County. The DA has six divisions:

- Branch Court Operations** – files felonies and conducts preliminary hearings. Prosecutes all misdemeanors in Orange County's four Adult Justice Centers and handles all juvenile offenders in the centralized Juvenile Court;
- Vertical Prosecutions/Violent Crimes** – includes DNA, Gangs, GRIP & Gang Injunctions, Homicide, Sexual Assault, and TARGET;
- General Felonies/Economic Crimes** – includes Consumer/Environmental Fraud, Family Protection, Major Narcotics, Felony Panel, Career Criminal, Insurance Fraud, Public Assistance Fraud, and Major Fraud;
- Special Projects** – includes DA Projects, High Profile Team, Law & Motion, and Special Prosecutions;
- Bureau of Investigation** – provides trial preparation assistance, serves as liaison to the local police agencies, and performs the initial investigation in selected cases; and
- Administrative Services** – provides the human resources, financial, office support, information technology, facilities, and research services to the Office.

DA utilizes a number of key systems including State and Countywide systems including:

- CMS – Case Management System: Used to track all criminal cases prosecuted by the DA;
- BILL – DNA Collection: Used to track the data of volunteers who have supplied a DNA sample;
- DNA: Used for crime scene DNA case tracking and DNA evidence tracking; and
- EDC – Electronic Directions for Complaints: Used by the County police agencies to upload Request for Complaints and supporting documentation.





## Information Technology Organization

DA's Information Technology is managed by the Manager of Information Technology, who reports to the Administrative Services Director. DA Information Technology employs seventeen (17) internal staff and is divided into the following three (3) functions:

1. Network,
2. Application Development, and
3. Helpdesk.

## SCOPE AND METHODOLOGY

Our audit evaluated selected general controls (see definition below) policies and procedures over the administration and use of DA's computing resources as of May 31, 2012. Our methodology included inquiry, auditor observation, and a review of policies and procedures over the following:

1. The adequacy of DA's security-related policies and procedures including security awareness and other security-related personnel policies and information security weaknesses are effectively remediated.
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.
3. The adequacy of DA'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.
5. The adequacy of general controls, primarily DA's policies and procedures, over disaster recovery/business continuity (assess DA's participation with CEO/IT contingency planning project) to help mitigate service interruptions and protect computing resources from environmental hazards.

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.

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. They are commonly categorized into three phases of a processing cycle:

- **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 EXCLUSIONS

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

- Application controls.
- Security settings for operating system, file directory, database, and remote access (telecommunication) other than reviewing policy and procedures for their appropriate configuration.
- Status of issues previously identified by other parties (e.g., Foundstone Audits).
- Compliance with laws and regulations applicable to DA including Criminal Justice Information Services (CJIS) Security Policy.
- Controls or processes performed by other parties including CEO/IT data center physical controls, network monitoring, etc.
- Security management control objectives including establishing a security management program, periodically assess and validate risks, monitor the effectiveness of the security program, and ensure that activities performed by external parties are adequately secure.
- Access control objectives including adequately protect information system boundaries, adequately protect sensitive system resources, and implement effective audit and monitoring capabilities.
- Configuration management control objectives including current configuration identification information is maintained, routinely monitor the configuration, update software on a timely basis, and appropriately document and approve emergency changes to the configuration.

## 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 District Attorney'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 District Attorney's operating procedures, accounting practices, and compliance with County policy.

## Acknowledgment

We appreciate the courtesy extended to us by the District Attorney personnel during our audit. If we can be of further assistance, please contact me directly at 834-5475 or Michael Goodwin, Senior Audit Manager at 834-6066.

## Attachments

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors  
Members, Audit Oversight Committee  
Lisa Bohan-Johnston, Director, Administrative Services, District Attorney  
Mike Kerr, Manager, Information Technology, District Attorney  
Foreperson, Grand Jury  
Susan Novak, Clerk of the Board of Supervisors





**Objective #1:** Evaluate the adequacy of DA's security-related policies and procedures including security awareness and other security-related personnel policies and information security weaknesses are effectively remediated.

## Work Performed

To accomplish this objective, we obtained and reviewed DA's security-related policies and procedures including security awareness and other security-related policies. Specifically, we interviewed DA IT staff; reviewed DA security-related policies and procedures including Computer Network Security Management, IT User Guide, Internet Use Policy Agreement, Securing Criminal Justice Information System data, Transmission of Data Security, Computer Network Access, Computer Network Passwords, and DA Employee Separation. In addition, we obtained third party security assessments and reviewed the status of issues and adequacy of the DA's responses.

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 can be held accountable for their actions; and
  - General and application controls.
  
- 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;
  - Nondisclosure 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.
  
- Issues identified by third party security assessments were effectively remediated.

## Conclusion

Based on the work performed, adequate security-related policies and procedures have been developed including security awareness and other security-related personnel policies and information security weaknesses were effectively remediated.

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



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

## Work Performed

To accomplish this objective, we audited general computer controls and processes over access to DA's computing resources located at **401 Civic Center** and **700 Civic Center** buildings. We reviewed system security settings for the District Attorney network. We discussed network system procedures with DA IT staff. We visited the rooms housing DA's computing resources located at 401 Civic Center and 700 Civic Center and observed selected controls for restricting access to DA computing resources. Our evaluation of controls and processes noted that:

- DA implemented adequate identification and authentication mechanisms including network system security settings for accessing DA's computing resources that were appropriate and complied with best practices as follows:
  - Minimum password length;
  - Number of days before system forces system password changes;
  - Number of times password must be changed before a password may be reused;
  - Number of incorrect logon attempts before the account is locked;
  - Length of lock out period; and
  - Length of time incorrect logon count is retained.
- DA implemented adequate authorization controls.
- Physical controls for restricting access to DA's computing resources located at 401 Civic Center and 700 Civic Center 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 card keys is documented and controlled; and
  - Workstations are logically locked when not in use.
- DA obtained third-party (Foundstone) security assessments and penetration testing between 2008 and 2010 on various applications. We obtained and reviewed the Foundstone assessments and the DA's response to issues identified in the assessments and noted that the DA took appropriate corrective action in response to the assessments.

## 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.

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



**Objective #3:** Evaluate the adequacy of DA'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 including review of project documentation for one sample change request/implementation. 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 (SDLC) 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 including: project request form, project kick-off meeting, meeting minutes, project plan, Gantt chart, and functional and technical specifications.
- 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.

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

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

## Work Performed

To accomplish this objective, we reviewed the DA's IT organization chart and job descriptions for the seventeen (17) 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 the utilization of an "open" systems architecture, 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 for system backup and monitoring; accordingly, no personnel are needed or assigned as System Programmers. No incompatible IT duties were noted in our review.

## 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 DA's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions and protect computing resources from environmental hazards.

## Work Performed

To accomplish this objective, we reviewed applicable policies and procedures for backup and recovery. We also determined the DA 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 DA's computing resources at the 401 Civic Center building and the 700 Civic Center building. 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 completed regularly;
  - The recovery process and back-up tapes were recently write tested as part of the Solano County recovery solution to ensure that they can be utilized if required;
  - The backup scheme allows the system to be restored within 24 hours of an incident;
  - On-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.
- DA was participating in the CEO/IT contingency planning project and is 18% complete with Phase One as of April 5, 2012. See [Finding #1](#) below.
- Controls to protect computing resources from environmental hazards at the room housing DA's computing resources at the 401 Civic Center building were adequate and included:
  - Access to the building is restricted to DA employees with visitor access via the receptionist;
  - Computer room is restricted to IT staff via badge reader;
  - Computer room has separate AC system with the building as backup;
  - Computer room has emergency power shut off;
  - Smoke, heat, and water detection devices are installed to provide early warning;
  - Automated fire extinguishing systems are installed;
  - Computer monitoring system sends email alerts for temperature changes;
  - 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;
  - Building is supported by a diesel backup generator that is tested monthly by OC Public Works;
  - Emergency lighting has been installed; and
  - Protection systems are maintained regularly.
- Controls to protect computing resources from environmental hazards at the room housing DA's computing resources at the 700 Civic Center building were adequate and included:
  - Access to the building is controlled by Orange County Sheriffs with visitor access via the receptionist;
  - Computer room is restricted to IT staff via badge reader;
  - Computer room has separate AC system with the building as backup;
  - Hand held fire extinguishers are located in strategic locations near the computers;
  - Computers are secured in rack mounts and bolted to the floor (case is locked with key in a lock box at 401 Civic Center);
  - Uninterrupted power supply (UPS) units are installed for all significant system components;



- Building is supported by a backup generator;
- 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 and protect computing resources from environmental hazards.

However, our audit disclosed one issue that impacts the CEO/IT business continuity planning documents. We identified **one (1) Control Finding** to improve and enhance controls and processes in addressing business continuity planning. The finding and recommendation is discussed below.

## Finding No. 1 – Need to Complete Business Continuity Planning Documents

### Summary

As of April 5, 2012, the DA has completed and submitted to CEO/IT about 18% of the County's Business Continuity Fundamental Plan Components documents for Phase One. **(Control Finding)**

### Details

A current and effective business continuity plan is necessary to ensure continued operations in the event of a disaster. To this end, the County created the County of Orange Business Continuity Program and tasked CEO/IT with managing this effort. CEO/IT divided the task into two phases: (1) business impact analysis and development of business continuity plan documents, and (2) testing of the plan documents and on-going maintenance of the plan documents. Currently, CEO/IT is coordinating with the County departments to complete the Phase One - Business Continuity Fundamental Plan Components (completion target was end of 2011) and to transition County departments into Phase Two - testing of the plan documents. As part of managing the project, CEO/IT purchased software to assist with the development of the documentation including the PrepareOC and RecoverOC web portals, templates and samples for the Business Continuity Fundamental Plan Components.

As of April 5, 2012, the DA has completed and submitted about 18% of the Business Continuity Fundamental Plan Components documents to CEO/IT. CEO/IT has received the following documents from the DA:

- Critical Business Process Listing (complete),
- Critical Process IT Dependency (complete), and
- Critical Business Process IT Dependency Recovery Strategies Identification (incomplete).

The following documents have not been submitted by DA:

- Delegations of Authority,
- Orders of Succession,
- RACI (Responsible, Accountable, Consulted, Informed) and Team Responsibilities/Detail,
- Logistics Tables (such as Alternate Facilities, IT Dependencies, Vital Records, Workforce Planning, and Vendors and Supporting Departments),
- Communication Tables,
- Critical Business Process Continuity Strategy Identification,
- Incident Response Workflow/Decision Matrix, and
- Incident Response Checklist.



Although the DA has substantially developed the policies and procedures to help mitigate service interruptions in the event of a disaster, the absence of these documents may impede DA from continuing/resuming normal business operations in an effective and timely manner. DA's delays to complete a consolidated business continuity document appear to be due to insufficient resources.

## **Recommendation No. 1**

DA continues to participate with the Countywide Business Continuity planning project and make it a priority to complete and submit the Business Continuity Fundamental Plan Components documents (Phase One).

## **District Attorney Management Response**

**Concur.** The DA has completed and submitted additional Business Continuity Fundamental Plan Components documents since the audit was conducted and will continue to make it a priority to complete the remainder of the required documents. In the interim, the office has substantially developed policies and procedures to mitigate service interruptions and is in a position to continue/resume normal business operations in an effective and timely manner.





## 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: District Attorney Management Response




TONY RACKAUCKAS  
DISTRICT ATTORNEY

## MEMO

OFFICE OF THE DISTRICT ATTORNEY

April 17, 2013

TO: Wilson Crider, CPA, CISA  
IT Audit Manager

FROM:  Lisa Bohan-Johnston  
Director, Administrative Services

SUBJECT: Confidential Draft Report on Information Technology Audit of District  
Attorney Computer General Controls

Thank you for the opportunity to review the draft audit and provide a response to the audit's recommendation.

### Recommendation No. 1

DA continues to participate with the Countywide Business Continuity planning project and make it a priority to complete and submit the Business Continuity Fundamental Plan Components documents (Phase One).

### District Attorney Management Response

Concur. The DA has completed and submitted additional Business Continuity Fundamental Plan Components documents since the audit was conducted and will continue to make it a priority to complete the remainder of the required documents. In the interim, the office has substantially developed policies and procedures to mitigate service interruptions and is in a position to continue/resume normal business operations in an effective and timely manner.

If you need any other information, please contact me at 714-347-8443 or at [Lisa.Bohan-Johnston@da.ocgov.com](mailto:Lisa.Bohan-Johnston@da.ocgov.com).

Thank you.

c: Michael Goodwin, Senior Audit Manager  
Michael Kerr, IT Manager