

Internal Audit Department

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

INFORMATION TECHNOLOGY AUDIT:

CHILD SUPPORT SERVICES COMPUTER GENERAL CONTROLS

Key Control Audit

As of January 31, 2013

We audited select computer general controls over the administration and use of Child Support Services' (CSS) 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 found that CSS partnered effectively with the County Executive Office/Information Technology in establishing, maintaining and monitoring the effectiveness, reliability and security of computer general controls. Our audit identified **one (1) Control Finding** regarding policies and procedures for securing vendor supplied accounts that Internal Audit subsequently verified was addressed prior to the issuance of the audit report.

AUDIT No: 1251

REPORT DATE: JUNE 20, 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



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

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes

Director

Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF, CGMA

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

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



OC Fraud Hotline (714) 834-3608



Transmittal Letter



Audit No. 1251 June 20, 2013

TO: Winnie Hewett, Interim Director
Child Support Services

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

SUBJECT: Information Technology Audit:
Child Support Services
Computer General Controls

We have completed an Information Technology Audit of Child Support Services - Computer General Controls as of January 31, 2013. We performed this audit in accordance with our *FY 2012-13 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.

Table of Contents



Information Technology Audit:
Child Support Services
Computer General Controls
Audit No. 1251

As of January 31, 2013

Transmittal Letter	i
OC Internal Auditor's Report	
OBJECTIVES	1
RESULTS	1
BACKGROUND	2
SCOPE AND METHODOLOGY	4
SCOPE EXCLUSIONS	4
Detailed Results, Findings, Recommendations and Management Responses	
Finding No. 1 – Need to Create Policy and Procedures for Vendor Supplied Accounts (Control Finding)	7
ATTACHMENT A: Report Item Classifications	11

OC Internal Auditor's Report



Audit No. 1251

June 20, 2013

TO: Winnie Hewett, Interim Director
Child Support Services

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

PH

SUBJECT: Information Technology Audit: Child Support Services
Computer General Controls

Audit Highlight

The Orange County Department of Child Support Services (CSS) provides professional cost-effective services to parents or caretakers of minor children. It offers solutions for parents including the establishment and enforcement of child support orders through exclusive enforcement tools, establishment of legal paternity through genetic testing, complete account maintenance, and customer service to assist customers every step of the way.

CSS is part of a statewide child support program where all California counties serve customers through the use of the Child Support Enforcement (CSE) system. CSE is operated by the State Department of Child Support Services and is the central database for child support case information. Through CSE, CSS gained efficiencies and greater consistencies in business practices for child support statewide.

We identified **one (1) Control Finding** regarding policies and procedures for vendor supplied accounts that IAD subsequently verified was addressed.

OBJECTIVES

In accordance with our *FY 2012-2013 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors, we conducted an Information Technology Audit of Child Support Services - 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 CSS'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 CSS'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 CSS'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 policies and procedures for vendor supplied accounts that Internal Audit subsequently verified was addressed prior to issuance of the audit report.

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 have been developed to help mitigate service interruptions. No findings were identified under this objective.

OC Internal Auditor's Report



The following table summarizes our finding and recommendation 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 (see Attachment A)	Finding and Page No. in Audit Report	Recommendation	Concurrence by Management?
1.	Control Finding	<u>Need to Create Policies and Procedures for Vendor Supplied Accounts</u> – CSS should formalize its procedures for securing vendor supplied accounts (pg. 7).	No recommendation is needed as sufficient corrective action was taken by CSS after our fieldwork was completed.	Yes

BACKGROUND

The Orange County Department of Child Support Services (CSS) provides professional cost-effective services to parents or caretakers of minor children. Its mission is *"To enhance the quality of life for children and families by establishing and enforcing court orders for the financial and medical support of children in an effective, efficient, and professional manner."* CSS offer solutions for parents including the establishment and enforcement of child support orders through exclusive enforcement tools, establishment of legal paternity through genetic testing, complete account maintenance, and exceptional customer service to assist customers every step of the way.

- Establishment of Court Orders for Financial and Medical Support – prerequisite for collecting child support is the establishment of a Support Order defined as all legally enforceable court orders, including orders for medical insurance.
- Enforcement of Court Orders for Support – staff utilize specialized enforcement tools and resources to assist parents in collecting child support: wage withholding; liens on real and personal property; intercepting of federal and state tax refunds; denial of passports, credit cards, and suspension of business, professional and driver's licenses.
- Establishment of Paternity – an initial step to obtain a support order for a child born to unmarried parents to ensure the same legal rights are provided to the child as to one born to married parents.
- Collection and Distribution of Payments – Distribution of child support payments occur through the State Disbursement Unit (SDU). CSS collaborates with the SDU to ensure accurate collection and disbursement of child support payments.

CSS is part of a statewide child support program where all California counties serve customers through the use of the Child Support Enforcement (CSE) system. CSE is operated by the **State Department of Child Support Services (DCSS)** and is the central database for child support case information. Through CSE, CSS gained efficiencies and greater consistencies in business practices for child support statewide. At the County level, CSS' information systems are administered and maintained by the **County Executive Office of Information Technology (CEO/IT)**. Improved efficiencies and customer service has been achieved through new or enhanced software applications developed and implemented by CSS.

CSS has a **budget of \$58.8 million with a staff of 626** organized into two areas:



- Court Operations including attorneys and support staff.
- Non-Court Operations which is divided into five areas:
 1. Case Management Operations,
 2. Performance Management & Improvement,
 3. Policy & Process Management,
 4. Research and Reporting, and
 5. Administrative Support Services & Information Technology.

Information Technology Organization

CSS's Information Technology is managed by the Manager of Information Technology, who reports to the Deputy Director of Administrative Services and Information Technology. CSS Information Technology employs eleven (11) internal staff and is divided into the following four (4) functions:

1. Application Services,
2. Security Administration,
3. Technical Support, and
4. Operations/Infrastructure.

CSS utilizes a number of key systems including State/Consortia systems:

- **CalWorks Information Network (CalWin)** – An online, real time State system supporting all major processing functions to administer California's public assistance programs.
- **Child Support Enforcement (CSE)** – State system database to facilitate the sharing of case management information between California counties and the SDU to centralize collection and distribution of child support funds.
- **State Distribution Unit (SDU)** – State system providing child support payment collection and distribution information.

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. 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 AND METHODOLOGY

Our audit evaluated policies and procedures over select general controls (see definition above) over the administration and use of CSS's computing resources as of January 31, 2013. Our methodology included inquiry, auditor observation, and limited testing of policies and procedures over the following:

1. The adequacy of CSS'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 CSS'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. CSS uses primarily State consortium system and off the shelf software.
4. The adequacy of segregation of duties within the IT function. We evaluated the roles and responsibilities of CSS 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 CSS'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 CSS 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 HIPAA, IRS, DMV, and DCCS Information Security.
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 since CSS' significant systems are either State or consortia.
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 adjust 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 Child Support Service'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 Child Support Service's operating procedures, accounting practices, and compliance with County policy.

Acknowledgment

We appreciate the courtesy extended to us by Child Support Services' personnel during our audit. If we can be of further assistance, please contact me directly at 834-5475 or Mike 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
Michael B. Giancola, County Executive Officer
Susan Johnston, Deputy Director, CSS/Administrative Services & Information Technology
Mahesh Patel, Deputy CEO and Chief Information Officer
KC Roestenberg, Director, Enterprise IT Shared Services
Tony Lucich, County Information Security Officer
Rachael Vargas, Manager, CSS/Information Technology
Foreperson, Grand Jury
Susan Novak, Clerk of the Board of Supervisors
Vavrinek, Trine, Day and Co., LLP, County External Auditor

Detailed Results, Findings, Recommendations and Management Responses



Objective #1: Evaluate the adequacy of CSS'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 CSS's security-related policies and procedures including security awareness and other security-related policies. Specifically, we interviewed CSS IT staff; reviewed CSS security-related policies and procedures including Government Risk and Compliance Matrix, CSS Agency Policy Matrix, DCSS Internal Safeguard Review Evaluation Matrix, and other CSS Policies and Procedures. In addition, we obtained a security vulnerability assessment performed by CEO/IT Security 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:
 - o Security risk assessment;
 - o Purpose, scope, roles, responsibilities, and compliance;
 - o Users can be held accountable for their actions; and
 - o General and application controls.
 - o CSS is subject to both *County IT Usage and IT Security Policy* requirements and a very detailed and comprehensive *Information Security Manual* from the California Department of Child Support Services.
 - o CSS provided security awareness training on Information Security and Privacy.
- Adequate security awareness and other security-related personnel policies are documented and address:
 - o Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors;
 - o Hiring, transfer, termination, and performance policies address security;
 - o Nondisclosure or security access agreements are required for employees and contractors assigned to work with sensitive information;
 - o Formal sanctions process is employed for personnel failing to comply with security policy and procedures;
 - o 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
 - o Employee training and professional development is provided and available to CSS staff.

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 CSS partnered effectively with California Department of Child Support Services and the 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.

Detailed Results, Findings, Recommendations and Management Responses



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

To accomplish this objective, we audited general computer controls and processes over access to CSS's computing resources located at the 1055 Main Street building. We reviewed system security settings for the CSS network. We discussed network system procedures with CSS IT Staff. We visited the room housing CSS's computing resources located at 1055 Main Street and observed selected controls for restricting access to CSS computing resources. We selected a sample of user access to verify access was authorized. We selected a sample of separated employees to verify their access was removed in a timely manner.

Our evaluation of controls and processes noted that:

- CSS implemented adequate identification and authentication mechanisms including network system security settings for accessing CSS's computing resources were appropriate and complied with best practices as follows:
 - o Minimum password length;
 - o Number of days before system forces system password changes;
 - o Number of times password must be changed before a password may be reused;
 - o Number of incorrect logon attempts before the account is locked;
 - o Length of lock out period; and
 - o Length of time incorrect logon count is retained.
- CSS implemented adequate authorization controls.
- Physical Controls for restricting access to CSS's computing resources located at 1055 Main Street were adequate and included:
 - o Computers reside in locked or otherwise restricted areas;
 - o Combinations, keys, or magnetic card keys are given to authorized personnel;
 - o Issuance of combinations, keys, or magnetic cards keys is documented and controlled; and
 - o Workstations are logically locked when not in use.
- CEO/IT Security Operations conducted a vulnerability assessment of the CSS network computing infrastructure. We reviewed the report that noted some concerns were identified. We noted that CSS took appropriate corrective action to remediate the concerns in response to the assessment.

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 regarding policies and procedures for vendor supplied accounts. We identified **one (1) Control Finding** to improve and enhance policies and procedures that Internal Audit subsequently verified was addressed. The finding is discussed below.

Finding No. 1 – Need to Create Policy and Procedures for Vendor Supplied Accounts

Summary

CSS did not have documented policies and procedures for securing vendor supplied accounts. **(Control Finding)**

Detailed Results, Findings, Recommendations and Management Responses



Details

Effective policies and procedures are necessary to ensure IT operational tasks are performed in a consistent manner. To this end, CSS did not have documented policies and procedures for securing vendor supplied accounts. This is critical when using off-the-shelf products that come with pre-set settings and configuration. Procedures should include deleting or disabling unnecessary accounts, requiring the changing of default passwords, and restricting access to system account passwords except when needed. Without these policies and procedures, an unauthorized individual may inappropriately use the vendor supplied accounts to access CSS computing resources.

Subsequent to the completion of our fieldwork, Internal Audit verified CSS had documented policies/procedures addressing the securing of vendor supplied accounts.

Recommendation No. 1

No recommendation is needed as sufficient corrective action was taken by CSS after our fieldwork was completed.

Child Support Services Management Response Concur.

Objective #3: Evaluate the adequacy of CSS'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 (1) 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:
 - o Roles, responsibilities, procedures, and documentation requirements.
 - o Review and approval of changes by management.
 - o SDLC methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system; and
 - o Appropriate system documentation.
 - o CSS uses primarily State consortium system and vendor supplied off-the-shelf software.
- 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.

Detailed Results, Findings, Recommendations and Management Responses



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

Work Performed

To accomplish this objective, we reviewed CSS' IT organization chart and job descriptions for the eleven (11) 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 CSS 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 CSS'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 CSS 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 CSS's computing resources at the 1055 Main Street building.

Our evaluation of controls and processes noted that:

- Written backup and recovery procedures were appropriate and addressed the following:
 - o Backups (system, data, full, incremental) are taken regularly;
 - o 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;
 - o The backup scheme allows the system to be restored to within 24 hours of the incident;
 - o On-site backup tapes are stored in secured, locked and fireproof facilities;
 - o Off-site backup tapes are stored in secured, locked and fireproof facilities;
 - o Backup tapes are rotated between on-site and off-site storage facilities; and
 - o Recovery procedures are documented.
- CSS was participating in the CEO/IT contingency planning project and is **100% complete** with Phase One as of February 1, 2013.
- Controls to protect computing resources from environmental hazards at the room housing CSS's computing resources at the 1055 Main Street building were adequate and included:
 - o Access to the building is restricted to CSS employees. Visitors may access via the receptionist;
 - o Computer room is restricted to IT staff via badge reader;
 - o Computer room has separate AC system with building as backup;

Detailed Results, Findings, Recommendations and Management Responses



- o Computer room has emergency power shut off;
- o Smoke, heat, and water detection devices are installed to provide early warning;
- o Automated fire extinguishing systems are installed;
- o Computer monitoring system sends email alerts - temperature;
- o Hand held fire extinguishers are located in strategic locations near the computer;
- o Raised flooring;
- o Computers are secured in rack mounts and bolted to the floor;
- o Uninterrupted power supply (UPS) units are installed for all significant system components;
- o Building is supported by a diesel backup generator; tested monthly by OCPW;
- o Emergency lighting has been installed; and
- o 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.

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



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.