INFORMATION TECHNOLOGY AUDIT:

Key Control Audit

OC PUBLIC WORKS COMPUTER GENERAL CONTROLS

As of June 30, 2013

We audited select computer general controls over the administration and use of OC Public Works' (OCPW) 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 OCPW 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 did not identify any reportable audit findings or recommendations. We commend Information Technology on their detailed policies and procedures over OCPW's IT general controls.

AUDIT NO: 1354
REPORT DATE: NOVEMBER 26, 2013

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

*Certified Information Systems Auditor

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

Independence Objectivity Integrity

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

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

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 1354 November 26, 2013

TO: Shane Silsby, Director
OC Public Works

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

SUBJECT: Information Technology Audit:
OC Public Works Computer General Controls

We have completed an Information Technology Audit of OC Public Works - Computer General Controls as of June 30, 2013. 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 4.

Table of Contents

Information Technology Audit:
OC Public Works Computer General Controls
Audit No. 1354

As of June 30, 2013

OC Internal Auditor's Report

Audit No. 1354 **NOVEMBER 26, 2013**

TO: Shane Silsby, Director
OC Public Works

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

SUBJECT: Information Technology Audit: OC Public Works
Computer General Controls

Audit Highlight

OC Public Works with a budget of **$464 million and 974 staff positions** accomplishes its mission and strategic objectives through a dedicated professional workforce that is organized around the department's six core service areas: flood protection, safe roads, community planning and development, facilities operation, including real estate management, and land acquisition, regional water quality management, and the Agricultural Commissioner. These six core functions support the three Strategic Initiatives adopted by the Board of Supervisors: Protecting Our Community, Building for the Future of Our Community, Promoting a Healthy Community.

OCPW Information Technology Services is managed by an IT Manager, who reports to the Administrative Services Director. The OCPW Information Technology department consists of thirty-three (33) staff providing the following functions: Network Services, Application Development & Support, Planning, Analysis & Review, and Desktop Services.

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 OC Public Works - 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. The objectives of our audit were to:

1. Evaluate the adequacy of OCPW'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 OCPW'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 OCPW'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. 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 have been developed to help mitigate service interruptions. No findings were identified under this objective.

BACKGROUND

OC Public Works has a budget of **$464 million and 974 staff positions** to accomplish its mission and strategic objectives through a dedicated professional workforce comprised of five major service areas. These service areas support the three Strategic Initiatives adopted by the Board of Supervisors: Protecting Our Community, Building for the Future of Our Community, Promoting a Healthy Community.

- **OC Engineering** consisting of: *OC Construction*, *OC Flood, OC Operations and Maintenance, OC Road, OC Survey, OC Watersheds* and *Project Management*.
- **OC Facilities & Real Estate** consisting of: *Architecture and Engineering Project Management, OC Facilities Operation, OC Fleet Services and Real Estate Services.*
- **OC Planning** consisting of: *OC Communities, OC Community Development* and *OC Planned Communities*.
- **OC Agricultural Commissioner** consisting of: *Agriculture Programs, Agriculture Commissioner/Sealer of Weights & Measures* and *Weights & Measures/Pesticide Regulation*.
- **Administration** consisting of: *Accounting Services, Central Quality Assurance, Finance Services, Human Resources, Information Technology Services, Procurement & Special Services* and *Strategic Planning and Communications*.

Information Technology Services

OCPW Information Technology Services is managed by an IT Manager, who reports to the Administrative Services Director. The OCPW Information Technology department consists of thirty-three (33) staff providing the following functions: Network Services, Application Development & Support, Planning, Analysis & Review, and Desktop Services. OCPW utilizes a number of systems including:

- Accounting Budget Data (ABD) – imports accounting and budget data from CAPS+ and allows user to do custom query
- Automated Permitting and Planning System (APPS) – automated permitting and planning system provides permitting, processing, planning, and accounting services for OC Planning
- EnergyCap – enterprise energy management software for utility bill processing and energy reporting
- Fleet Focus – enterprise system to assist OCPW Transportation manage fleet vehicles including assets, maintenance, fueling, and rental (pool)
- Flagship Billing System – assists OCPW Transportation with allocating costs to departments for use of fleet vehicles
- ProgPay – construction bid and payment management system
- Footprints – IT service management software which allows end-user to create service requests and incident reports for IT related work

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, processing and output. This audit does not include application controls.

SCOPE AND METHODOLOGY

Our audit evaluated policies and procedures over select general controls (see definition above) over the administration and use of OCPW's computing resources as of June 30, 2013. Our methodology included inquiry, auditor observation, and limited testing of policies and procedures over the following:

1. The adequacy of OCPW'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 OCPW'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 OCPW 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 OCPW'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 OCPW 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 PCI.
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 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 OC Public Works' 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 OC Public Works' operating procedures, accounting practices, and compliance with County policy.

Acknowledgment

We appreciate the courtesy extended to us by OC Public Works' 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
Mark Denny, Chief Operating Officer
Mary Fitzgerald, Director, OCPW/Administration
Bob Berg, Manager, OCPW/Information Technology Services
Randi Dunlap, Policy and Compliance Manager, OCPW
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 OCPW'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 OCPW's security-related policies and procedures including security awareness and other security-related policies. Specifically, we interviewed OCPW IT staff; reviewed OCPW security-related policies and procedures including Account Management Procedures, Account Request Form, OC Public Works IT Usage Policy, OC Public Works: Information Technology Services Operations Manual, OC Public Works IT Security Management, and other OC Public Works Policies and Procedures. In addition, we obtained a security vulnerability assessment performed by Trustwave 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 can be held accountable for their actions;
  - OCPW is subject to both *County IT Usage and IT Security Policy* requirements; and
  - OCPW 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;
  - 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 is provided and available to OCPW staff.

- Trustwave conducted a vulnerability assessment of the OCPW credit card environment. We reviewed the report and noted no failing vulnerabilities were identified.

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 OCPW 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

To accomplish this objective, we audited general computer controls and processes over access to OCPW's computing resources located at the 300 North Flower Street building. We reviewed system security settings for the OCPW network. We discussed network system procedures with OCPW IT Staff. We visited the room housing OCPW's computing resources located at 300 North Flower Street and observed selected controls for restricting access to OCPW 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:

- OCPW implemented adequate identification and authentication mechanisms including network system security settings for accessing OCPW's computing resources 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.

- OCPW implemented adequate authorization controls.

- Physical Controls for restricting access to OCPW's computing resources located at 300 North Flower Street 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 OCPW's network was authorized and adequately documented.

- Access to OCPW's network for separated employees was removed on a timely basis.

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.

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

Objective #3: Evaluate the adequacy of OCPW'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:
  - Roles, responsibilities, procedures, and documentation requirements.
  - Review and approval of changes by management.
  - 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.

- 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 have 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 OCPW's IT organization chart and job descriptions for the thirty-three (33) 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 OCPW 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. 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 OCPW'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 OCPW 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 OCPW's computing resources at the 300 North Flower Street 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 taken 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 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.

- OCPW was participating in the CEO/IT contingency planning project and is **100% complete** with Phase One as of August 30, 2013.

- Controls to protect computing resources from environmental hazards at the room housing OCPW's computing resources at the 300 North Flower Street building were adequate and included:
  - Access to the building is restricted to OCPW employees. Visitors may access via the receptionist;
  - Computer room is restricted to IT staff via badge reader;
  - Computer room has separate AC system with 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;
  - 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; 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.

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.