ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

INFORMATION TECHNOLOGY AUDIT:

JOHN WAYNE AIRPORT COMPUTER GENERAL CONTROLS

As of May 31, 2015

Audit Number 1444
Report Date: October 15, 2015

ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

Eric H. Woolery, CPA

Orange County Auditor-Controller

Toni Smart, CPA	**Director, Internal Audit**
Michael Goodwin, CPA, CIA	**Assistant Director**
Wilson Crider, CPA, CISA	**Audit Manager**

12 Civic Center Plaza, Room 200

Santa Ana, CA 92701

Auditor-Controller Web Site

www.ac.ocgov.com

ERIC H. WOOLERY, CPA
AUDITOR-CONTROLLER

Transmittal Letter

Audit No. 1444

October 15, 2015

TO: Lawrence G. Serafini, Acting Airport Director
John Wayne Airport

SUBJECT: Information Technology Audit:
John Wayne Airport Computer General Controls

We have completed our Information Technology Audit of John Wayne Airport Computer General Controls as of May 31, 2015. Our final report is attached for your review.

I submit an **Audit Status Report** quarterly to the Audit Oversight Committee (AOC) and a monthly report to the Board of Supervisors (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. Although there were no findings and recommendations in this audit, the results of this audit will be included in a future status report to the AOC and BOS.

Additionally, we will request your department to complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

Toni Smart, CPA, Director
Auditor-Controller Internal Audit Division

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Eric Woolery, Auditor-Controller
Frank Kim, County Executive Officer
Mark Denny, Chief Operating Officer
Jessica O'Hare, Assistant to the Chief Operating Officer
Tim Harris, Chief Technology Officer, JWA
Kenneth Wong, Manager, JWA/Quality Assurance & Compliance
Foreperson, Grand Jury
Robin Stieler, Interim Clerk of the Board of Supervisors
Macias Gini & O'Connell LLP, County External Auditor

Table of Contents

Information Technology Audit:
John Wayne Airport Computer General Controls
Audit No. 1444

As of May 31, 2015

Internal Auditor's Report

Audit No. 1444 **October 15, 2015**

TO: Lawrence G. Serafini, Acting Airport Director
John Wayne Airport

FROM: Toni Smart, CPA, Director
Auditor-Controller Internal Audit Division

SUBJECT: Information Technology Audit:
John Wayne Airport Computer General Controls

OBJECTIVES

We conducted an Information Technology Audit of John Wayne Airport 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 JWA'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 JWA'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 implemented or subsequently modified;
4. Evaluate whether segregation of duties exists within the IT function; and
5. Evaluate the adequacy of JWA'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 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

John Wayne Airport, Orange County (JWA), owned and operated by the County of Orange, is the only commercial service airport in Orange County, California. It is located approximately 35 miles south of Los Angeles, between the cities of Costa Mesa, Irvine, and Newport Beach. The service area includes more than three million people within the 34 cities and unincorporated areas of Orange County. In 2014, more than nine million passengers were served.

John Wayne Airport plays a unique and crucial role in the Orange County community. It is the only airport in Orange County that provides commercial passenger and air-cargo service and is the primary provider of general aviation services and facilities in the county. It is home to local law enforcement air operations and to medical/mercy flights. JWA is the gateway through which millions of passengers travel each year to their homes, their families, their vacations, and their businesses.

Information Technology Services

JWA Information Technology is managed by its Chief Technology Officer, who reports to the Deputy Airport Director, Facilities. The JWA Information Technology department consists of approximately eleven staff organized into two groups:

- Service Group providing end user, desktop, telephone support, and Common Use Passenger Processing (CUPPs) application support, and
- Operations Group providing server, network, IT security, IT contract management, and Parking and Access Revenue Control System (PARCS) application support.

JWA utilizes a number of systems including:

- Common Use Passenger Processing (CUPPs)
- Parking and Access Revenue Control System (PARCS)

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 over the administration and use of JWA's computing resources as of May 31, 2015. Our methodology included inquiry, auditor observation, and limited testing of policies and procedures. Our audit was limited to reviewing written policies and procedures in the areas of security, user access and physical access controls, configuration/change management controls, segregation of duties within the IT function, and disaster recovery/business continuity. To accomplish our scope, we obtained an understanding of selected JWA general controls and compared them with the Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM) identified control objectives.

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

1. Application controls. This audit included only computer general controls.
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 Federal Aviation Administration (FAA) and Payment Card Industry Data Security Standards (PCI DSS).
4. Controls or processes performed by other parties including CEO/IT data center controls, network monitoring, intrusion/detection, firewall, remote access, etc.
5. Security management controls provided at the County level including establishing an entity-wide security management program, periodically assessing and validating risks, and monitoring the effectiveness of the County security program.
6. Access control objectives provided at the County level including adequately protecting information system boundaries, resources, and implementing effective audit and monitoring capabilities.
7. Configuration management controls including maintaining current configuration identification information and routinely monitoring configurations.
8. Contingency planning control objectives managed at the County level including developing and documenting a comprehensive contingency plan and periodically testing the contingency plan and adjusting it as appropriate.
9. We did not assess all control techniques or perform all potential audit procedures identified in FISCAM. Internal Audit made a determination of which general controls were included in the audit.

FOLLOW-UP PROCESS

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.

Because there were no findings and recommendations contained in this report, no Follow-Up Audits are needed.

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 JWA'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 JWA's operating procedures, accounting practices, and compliance with County policy.

The Auditor-Controller Internal Audit Division is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations.

ACKNOWLEDGEMENT

We appreciate the courtesy extended to us by the personnel at John Wayne Airport during our audit. If you have any questions regarding our information technology audit, please contact me directly at 834-5442, or Michael Goodwin, Assistant Director at 834-6066.

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

Work Performed

We obtained and reviewed JWA's security-related policies and procedures including security awareness and other security-related policies. Specifically, we interviewed JWA IT staff; reviewed JWA security-related policies and procedures including Information Technology Usage Policy, JWA Administrative Policies and Procedures Manual: Employee Separation, PCI DSS Information Security Policy, County IT Security Policy, and other JWA policies and procedures. In addition, we obtained the most recent PCI DSS security assessments performed by Coalfire Systems, Inc. and reviewed the identification of security weaknesses and remediation of the issues.

Our evaluation of the policies and procedures noted that:

- Policies relating to hiring and separation addressed the following:
  - Computer usage policy,
  - Security agreement/confidentiality statement,
  - Return of property, keys, and identification cards, and
  - Notification to security management of separation and prompt revocation of system access.

- System monitoring procedures addressed the following:
  - Potential security violations are recorded by the system;
  - Potential security violations are reviewed on a regular basis by security administration;
  - Potential security violations are investigated and cleared;
  - Potential security violations are the basis for adjustments to security; and
  - Summarized potential security violation information is regularly reported to management for appropriate action.

- Coalfire Systems, Inc. conducted security assessments of the JWA credit card environment. We reviewed the reports and noted no reportable issues 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. No findings or recommendations were identified under this audit objective.

Objective #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.

Work Performed
We audited general computer controls and processes over access to JWA's computing resources. We reviewed system security settings for the JWA network. We discussed network system procedures with JWA IT Staff. We visited the rooms housing JWA's computing resources and observed selected controls for restricting access to JWA's 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:

- JWA implemented adequate identification and authentication mechanisms including network system security settings for accessing JWA's computing resources which were appropriate in the following areas:
  - 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.

- JWA implemented adequate authorization controls.
  - Access to JWA's network was authorized and adequately documented.
  - Access to JWA's network for separated employees was removed on a timely basis.

- Physical Controls for restricting access to JWA's computing resources were adequate and included:
  - Computers reside in locked or otherwise restricted areas;
  - Combinations, keys, or magnetic card keys are given to authorized personnel; and
  - Issuance of combinations, keys, or magnetic cards keys is documented and controlled.

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. No findings or recommendations were identified under this audit objective.

Objective #3: Evaluate the adequacy of JWA'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 implemented or subsequently modified.

Work Performed
We reviewed policies and procedures over configuration management. We reviewed written procedures for implementing new systems and modifications to systems from request to installation.

Our evaluation of policies and procedures noted that:

- Configuration management policies and procedures are developed and address the following:
  - 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.

- 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 implemented or as a result of subsequent modifications. No findings or recommendations were identified under this audit objective.

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

Work Performed
We reviewed JWA's IT organization chart and job descriptions for the eleven 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 JWA 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, adequate segregation of duties exists in the IT function. No findings or recommendations were identified under this audit objective.

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

Work Performed

We reviewed applicable policies and procedures for backup and recovery. We also determined whether JWA 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 JWA's computing resources. Our evaluation of controls and processes noted the following:

- JWA's information technology infrastructure was designed to provide redundancy between the three computing centers. We determined this architecture was sufficient to provide continuous computer operations in the event of a single failure at any one of the computing centers. The rollover function has proven effective for JWA during prior network upgrades and rollouts. A schedule for future rollover tests is anticipated to be developed by JWA in January 2016.

- Although JWA is participating in the CEO/IT contingency planning project, JWA must comply with FAA regulations (more robust) that require an Airport Emergency Operations Plan which differs from the County. Therefore, the FAA requirements should supersede the County's contingency.

- Controls to protect computing resources from environmental hazards at the rooms housing JWA's computing resources included:
  - Access to the rooms is restricted to certain authorized JWA employees. Visitors may access via escort;
  - Computer rooms are restricted to IT staff via badge reader; computer room is separate from the employee work areas; computer room operates 24 hours a day/seven days a week;
  - Computer room doors are alarmed and monitored by Sheriff staff at the airport operations center;
  - Computer rooms access points at the terminal are video captured;
  - Computer rooms have separate air conditioning systems with separate backup systems;
  - Computer rooms have emergency power shut off via uninterrupted power supply (UPS);
  - Automated fire extinguishing systems (water pipe) are installed;
  - Fire suppression systems are activated by heat sensors;
  - Data center environmental sensors are tied to a building system and monitored by JWA facility staff;
  - Computers are secured in rack mounts;
  - UPS units are installed for all significant system components;
  - Computer rooms are supported by building diesel generators; tested monthly by JWA maintenance staff; and
  - Fire system maintained regularly by the vendor. Other systems including AC are maintained by JWA maintenance staff.

Conclusion

Based on the work performed, adequate policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions. No findings or recommendations were identified under this audit objective.

ATTACHMENT A: Report Item Classifications

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

- **Critical Control Weaknesses:**
  These are Audit Findings or a combination of Auditing Findings that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise the Department's or County's reputation for integrity. Management is expected to address Critical Control Weaknesses brought to their attention immediately.

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

- **Control Findings:**
  These are 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.