PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: John Wayne Airport Selected IT General Controls

For the Year Ended
December 31, 2019

Audit No. 1941
Report Date: December 17, 2020

Number of Recommendations

1	Critical Control Weaknesses
2	Significant Control Weaknesses
6	Control Findings

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
John Wayne Airport Selected IT General Controls

December 17, 2020

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of John Wayne Airport selected IT general controls for the year ended December 31, 2019.
RESULTS	• We concluded controls over regular and privileged logical access should be improved. • We concluded controls over deprovisioning access to critical systems should be improved. • We concluded controls over physical access to IT assets should be improved. • We concluded controls over data backup and data recovery should be improved. • We concluded controls over change management were sufficient to provide adequate protection of critical systems.
RISKS	As a result of our findings, potential risks include: • Unauthorized logical access to, and exposure of data. • Unauthorized physical access to IT assets. • Inability to quickly recover systems and data in the event of a disaster.
NUMBER OF RECOMMENDATIONS 1 CRITICAL CONTROL WEAKNESSES 2 SIGNIFICANT CONTROL WEAKNESSES 6 CONTROL FINDINGS	Opportunities for enhancing internal control include: • Periodically changing passwords. • Performing periodic user access reviews. • Performing an IT server room badge access review. • Ensuring changes are appropriately categorized and testing is documented. • Performing periodic tests of data backup media for recoverability and considering storage alternatives.

Report suspected fraud, or misuse of County resources by vendors, contractors, or County employees to 714.834.3608

AUDIT NO. 1941

INTERNAL AUDIT DEPARTMENT

Audit No. 1941

December 17, 2020

To: Barry Rondinella
John Wayne Airport Director

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Subject: Information Technology Audit: John Wayne Airport Selected IT General Controls

We have completed an Information Technology Audit of selected information technology general controls administered by John Wayne Airport (JWA) for the year ended December 31, 2019. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 7, 8 and 9 immediately follow this letter. Results for the remaining findings are included in Appendix A (which is redacted from public release) and additional information including background and our objectives, scope, and methodology are included in Appendix B.

JWA concurred with all our recommendations and the Internal Audit Department considers management's response appropriate to the recommendations in this report.

We will include the results of this audit in a future status report submitted quarterly to the Audit Oversight Committee and the Board of Supervisors. In addition, we will request your department complete a Customer Survey of Audit Services, which you will receive shortly after the distribution of our final report.

We appreciate the courtesy extended to us by John Wayne Airport personnel during our audit. If you have any questions, please contact me at 714.834.5442 or Assistant Director Scott Suzuki at 714.834.5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
John Wayne Airport Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Eide Bailly LLP, County External Auditor

RESULTS

Business Process & Internal Control Strengths

Business process and internal control strengths noted during our audit include:

- ✓ Strong badge security over secure areas of the airport, including badge checkpoints by guards at critical access points.
- ✓ Data backup is completed and properly captures critical data across JWA systems and network.
- ✓ Two authorization signoffs are required on all change control request forms.
- ✓ IT incidents and access requests are appropriately recorded and tracked in an incident management system.
- ✓ Full-time extra help IT security administrator staffed to address cybersecurity needs.

Finding No. 1

Removed due to the sensitive nature of the finding.

Finding No. 2

Removed due to the sensitive nature of the finding.

Finding No. 3

Removed due to the sensitive nature of the finding.

Finding No. 4

Removed due to the sensitive nature of the finding.

Finding No. 5

Removed due to the sensitive nature of the finding.

Finding No. 6

Removed due to the sensitive nature of the finding.

FINDING NO. 7	**Testing Documentation** JWA provided us copies of the change control forms that outlined testing and backout plans. While JWA asserted changes were properly tested, none of the six changes reviewed (100%) had detailed documentation to confirm that changes were tested prior to deployment.
CATEGORY	**Control Finding**
RISK	Lack of documenting testing results for changes increases the risk of not being able to reference prior testing details if the change does not function properly in production.
RECOMMENDATION	JWA management ensure test results are appropriately documented prior to deploying the change into production.
MANAGEMENT RESPONSE	**Concurs.** JWA Corrective Action JWA IT has modified the existing Change Control form with copy that requires the submitter to explicitly state the success or failure of test results as of May 2020.

FINDING NO. 8	**Change Control Form Change Category** While JWA utilized change control forms to document change requests, the forms lacked change category details to appropriately identify the type of change requested. Change category details provide key information to identify whether the requested change is a break fix, enhancement, upgrade, code change, etc., in order to appropriately allocate resources for the change.
CATEGORY	**Control Finding**
RISK	Lack of change category details could result in misallocation of resources, such as staffing and hours, for the change requested.
RECOMMENDATION	JWA management revise the change control form to require additional change category details.
MANAGEMENT RESPONSE	**Concurs**. JWA Corrective Action JWA IT will revise the change control form to require additional change category details by adding “change category” field to form with these values (1) break fix; (2) enhancement; (3) code change; (4) patch by 10/15/2020

FINDING NO. 9

Department IT Policies & Procedures

While JWA has strong IT policy and procedures in areas pertaining to Payment Card Industry Data Security Standard (PCI-DSS) compliance, they lacked such policy and procedures governing the administrative IT business processes over critical systems such as:

- Privileged user access rights management process, including provisioning and deprovisioning.
- Monitoring and maintaining appropriate access to JWA IT server rooms.

CATEGORY

Control Finding

RISK

Lack of IT policy and procedures can result in a lack of consistent understanding of IT business processes, cybersecurity violations, and delayed implementation of systems.

RECOMMENDATION

JWA management develop comprehensive IT policy and procedures that govern privileged user access management and physical access management to the JWA server rooms.

MANAGEMENT RESPONSE

Concurs. JWA Corrective Action

- JWA IT will modify the existing "JWA IT User Management Procedure v2.1" document to reflect a section for policy and procedure for privileged user access management and physical access management to server rooms by 12/5/2020.
- JWA OPERATIONS (badging) will create a process document to formalize the monitoring and maintaining of appropriate access to JWA IT server rooms by 12/5/2020.

AUDIT TEAM		
	Scott Suzuki, CPA, CIA, CISA, CFE	Assistant Director
	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Scott Kim, CPA, CISA, CFE	IT Audit Manager I
	Stephany Pantigoso	Senior Auditor

APPENDIX A: RESTRICTED INFORMATION

Content in Appendix A has been removed from this report due to the sensitive nature of the specific findings.

APPENDIX B: ADDITIONAL INFORMATION

OBJECTIVES

Our audit objectives were to determine if John Wayne Airport selected IT general controls:

1. Provide reasonable assurance that regular and privileged access to critical systems is limited to authorized individuals.
2. Provide reasonable assurance that regular and privileged access to critical systems is disabled timely.
3. Provide reasonable assurance that physical access to IT server rooms or other sensitive IT areas is limited to authorized individuals.
4. Provide reasonable assurance that data backups are complete and data can be recovered in an emergency.
5. Provide reasonable assurance that changes to critical systems are authorized and appropriately tested before being deployed into production.

SCOPE & METHODOLOGY

Our audit scope was limited to high risk information technology general controls over logical access, change management, physical access, and data backup and recovery at JWA for the year ended December 31, 2019. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.

EXCLUSIONS

We did not examine application controls or any processes that involve external parties such as OCIT or systems managed by the State of California, nor any services/activities performed or provided by the County or state's third-party vendors. In addition, we did not examine systems or controls that directly involved Payment Card Industry Data Security Standard (PCI-DSS) assessments such as Parking and Access Revenue Control System (PARCS) and Common Use Passenger Processing (CUPPS) systems.

PRIOR AUDIT COVERAGE

We noted one audit of this scope has been issued for John Wayne Airport in the last 10 years.

BACKGROUND

John Wayne Airport (JWA), owned and operated by the County of Orange, 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, families, vacations, and businesses.

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY

We performed this audit in accordance with the FY 2019-20 Audit Plan and Risk Assessment approved by the Audit Oversight Committee (AOC) and the Board of Supervisors (Board).

PROFESSIONAL STANDARDS

Our audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.

FOLLOW-UP PROCESS

In accordance with professional standards, the Internal Audit Department has a process to follow-up on its recommendations. A first follow-up audit will generally begin six months after release of the initial report.

The AOC and Board expect that audit recommendations will typically be implemented within six months or sooner for significant and higher risk issues. A second follow-up audit will generally begin six months after release of the first follow-up audit report, by which time all audit recommendations are expected to be implemented. Any audit recommendations not implemented after the second follow-up audit will be brought to the attention of the AOC at its next scheduled meeting.

A Follow-Up Audit Report Form is attached and is required to be returned to the Internal Audit Department approximately six months from the date of this report in order to facilitate the follow-up audit process.

MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL

In accordance with the Auditor-Controller's County Accounting Manual No. 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." Internal control should be continuously evaluated by management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating internal control is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. Our audit complements but does not substitute for department management's continuing emphasis on control activities and monitoring of control risks.

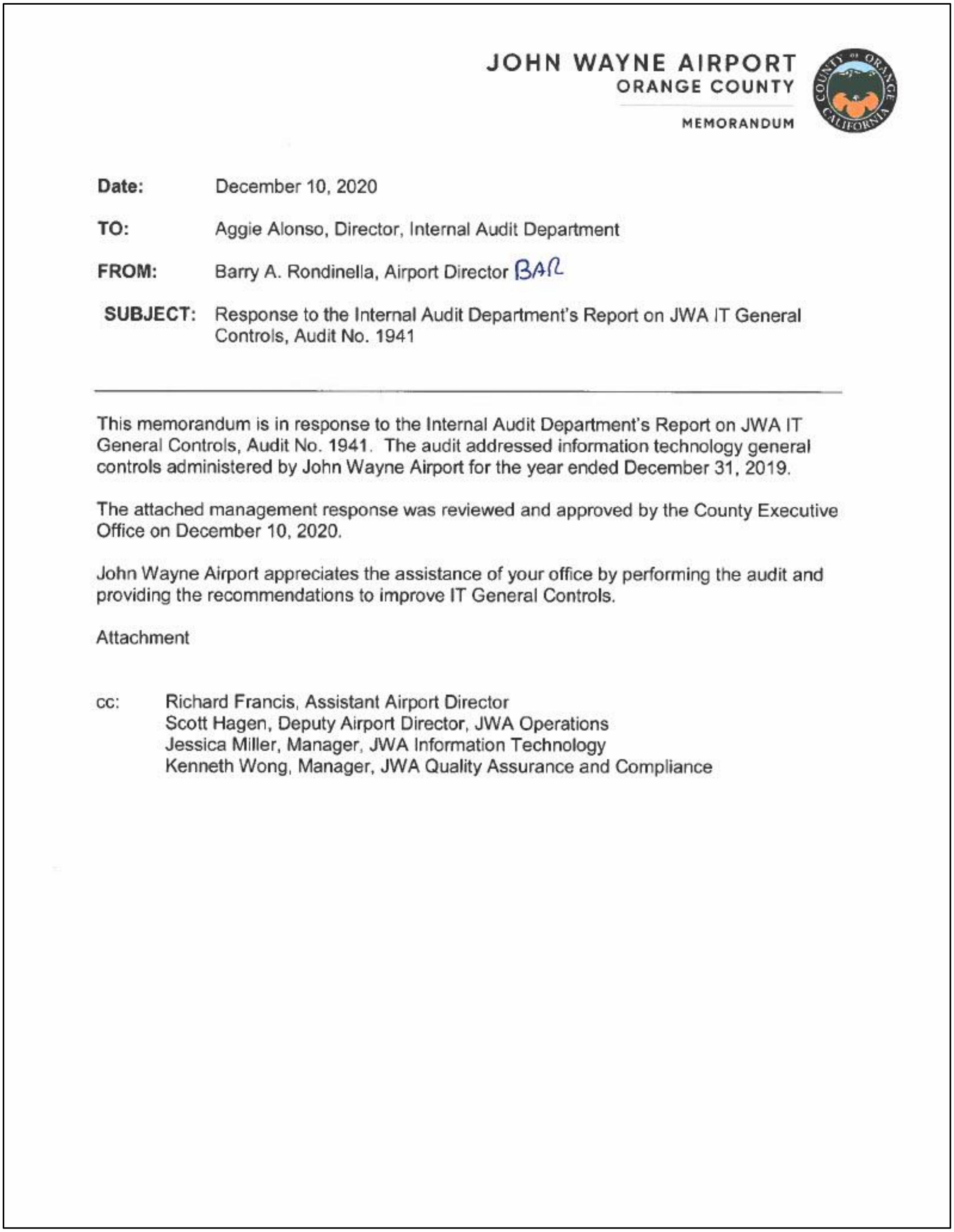
INTERNAL CONTROL LIMITATIONS

Because of inherent limitations in any system of internal control, 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 department's operating procedures, accounting practices, and compliance with County policy.

APPENDIX C: REPORT ITEM CLASSIFICATION

Critical Control Weakness	Significant Control Weakness	Control Finding
These are audit findings or a combination of audit 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 its attention immediately.	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.	These are audit findings concerning the effectiveness of internal control, compliance issues, or efficiency issues that require management's corrective action to implement or enhance processes and internal control. **Control Findings** are expected to be addressed within our follow-up process of six months, but no later than twelve months.

APPENDIX D: JOHN WAYNE AIRPORT MANAGEMENT RESPONSE



JOHN WAYNE AIRPORT
ORANGE COUNTY
MEMORANDUM

Date: December 10, 2020

TO: Aggie Alonso, Director, Internal Audit Department

FROM: Barry A. Rondinella, Airport Director BAR

SUBJECT: Response to the Internal Audit Department's Report on JWA IT General Controls, Audit No. 1941

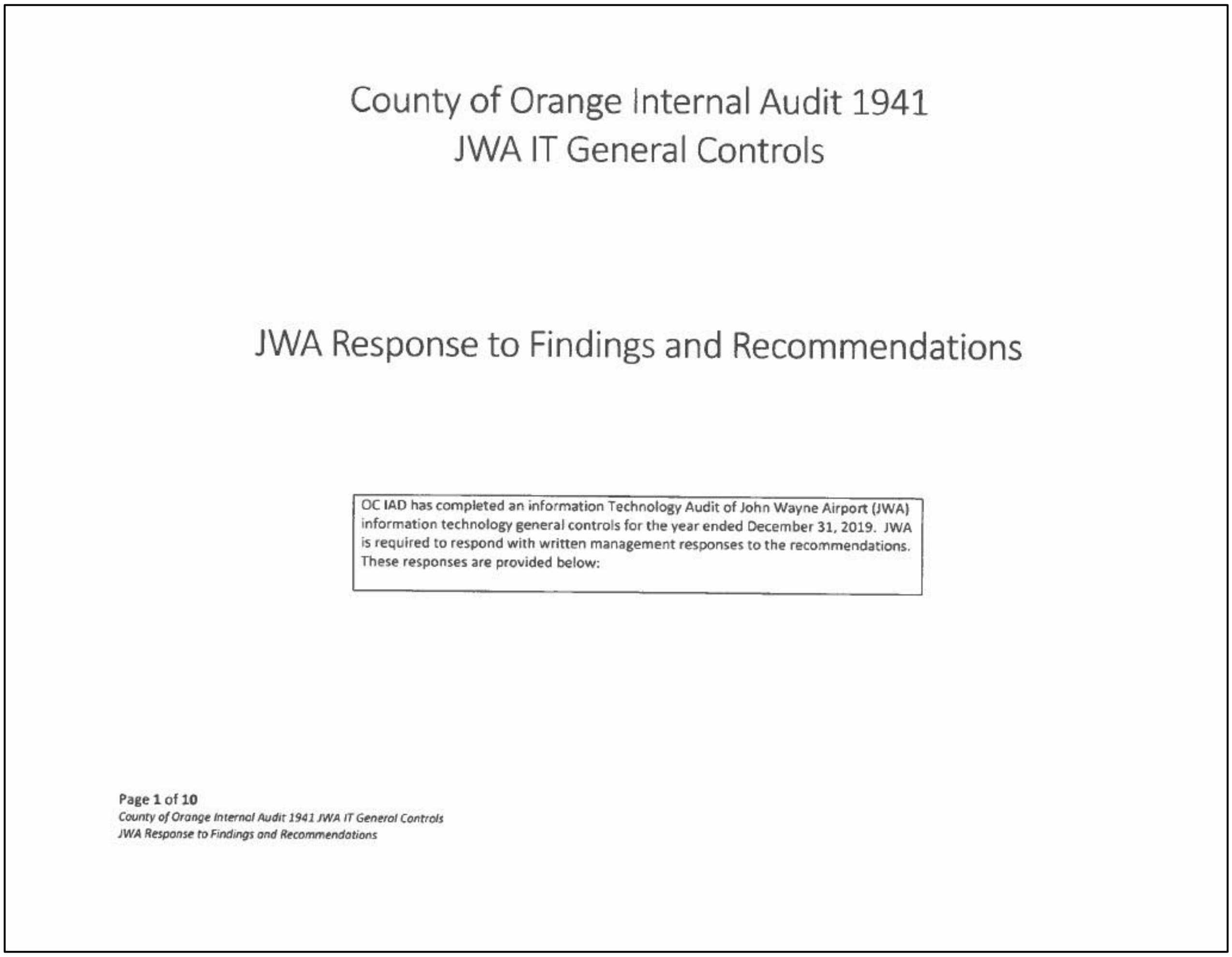
This memorandum is in response to the Internal Audit Department's Report on JWA IT General Controls, Audit No. 1941. The audit addressed information technology general controls administered by John Wayne Airport for the year ended December 31, 2019.

The attached management response was reviewed and approved by the County Executive Office on December 10, 2020.

John Wayne Airport appreciates the assistance of your office by performing the audit and providing the recommendations to improve IT General Controls.

Attachment

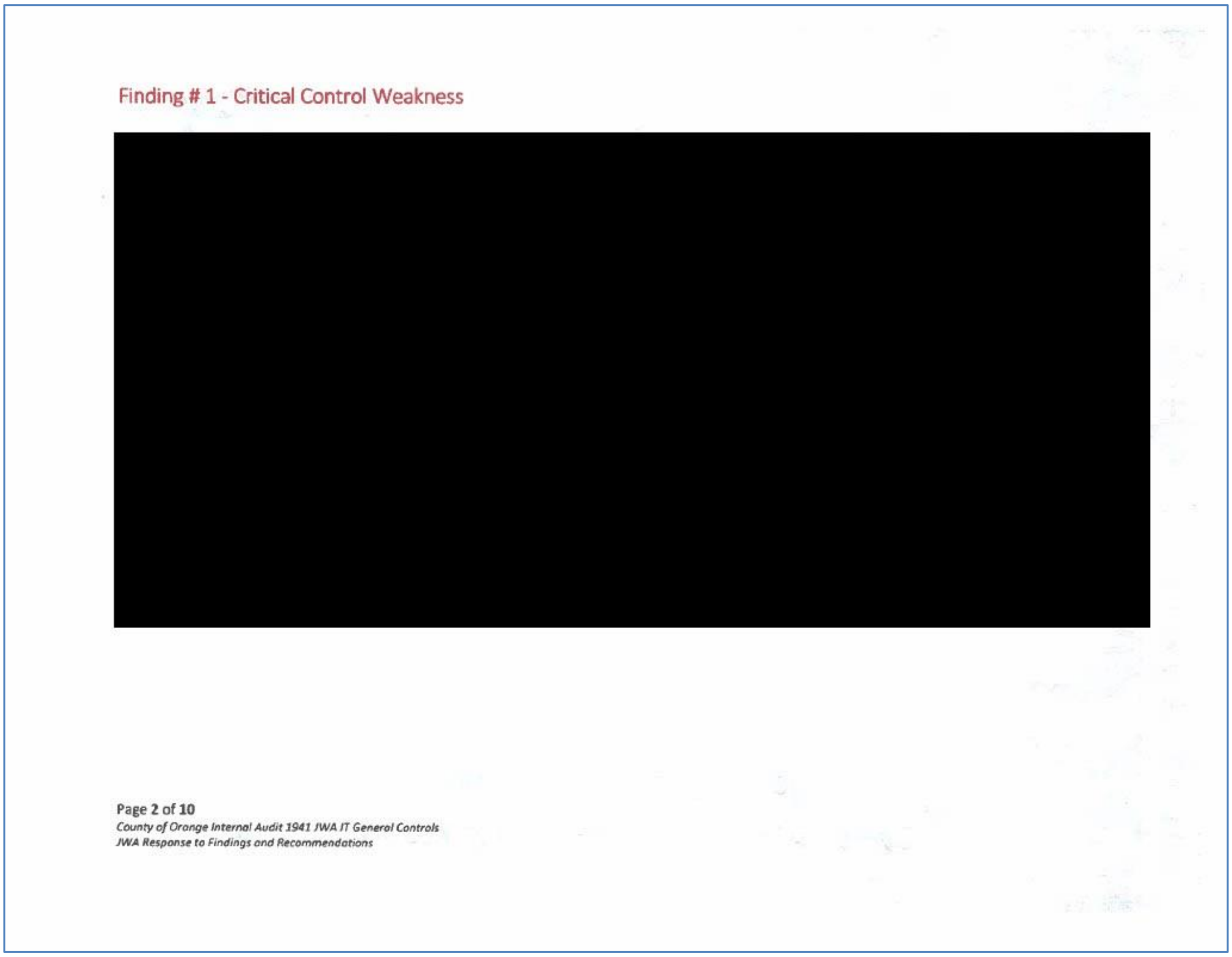
cc: Richard Francis, Assistant Airport Director
Scott Hagen, Deputy Airport Director, JWA Operations
Jessica Miller, Manager, JWA Information Technology
Kenneth Wong, Manager, JWA Quality Assurance and Compliance



County of Orange Internal Audit 1941
JWA IT General Controls

JWA Response to Findings and Recommendations

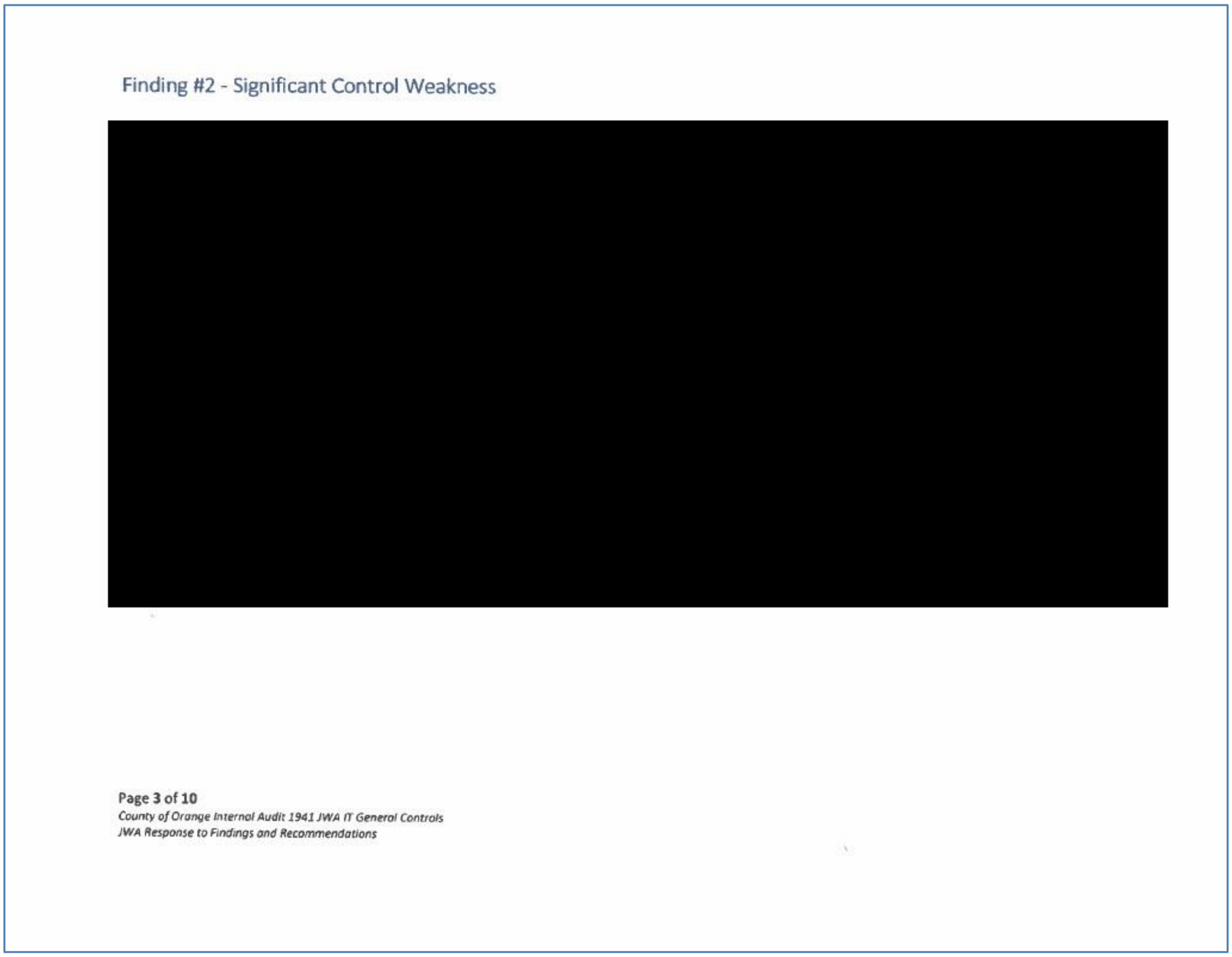
OC IAD has completed an information Technology Audit of John Wayne Airport (JWA) information technology general controls for the year ended December 31, 2019. JWA is required to respond with written management responses to the recommendations. These responses are provided below:



Finding # 1 - Critical Control Weakness

[redacted]

Page 2 of 10
County of Orange Internal Audit 1941 JWA IT General Controls
JWA Response to Findings and Recommendations



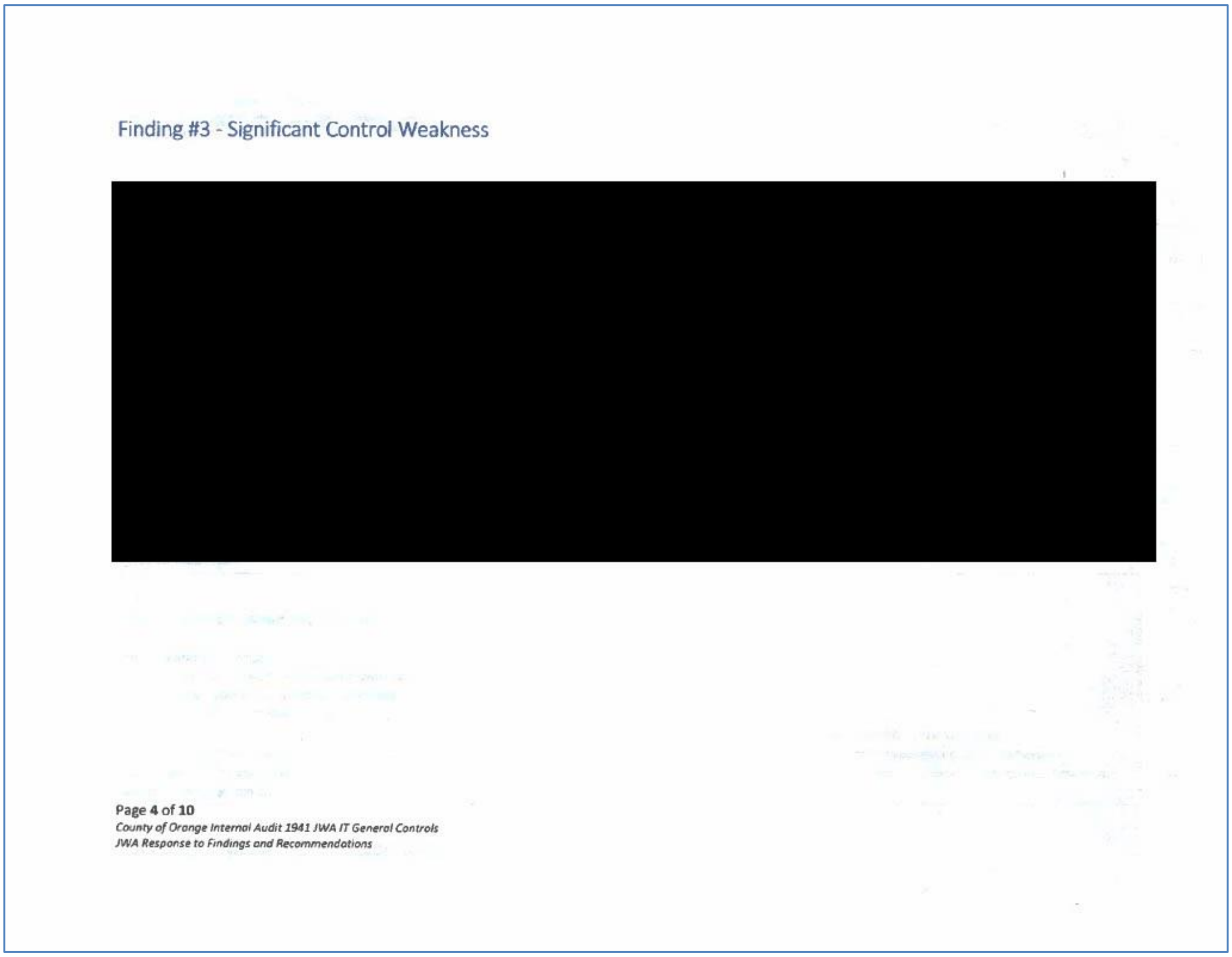
Finding #2 - Significant Control Weakness

[redacted]

Page 3 of 10

County of Orange Internal Audit 1941 JWA IT General Controls

JWA Response to Findings and Recommendations



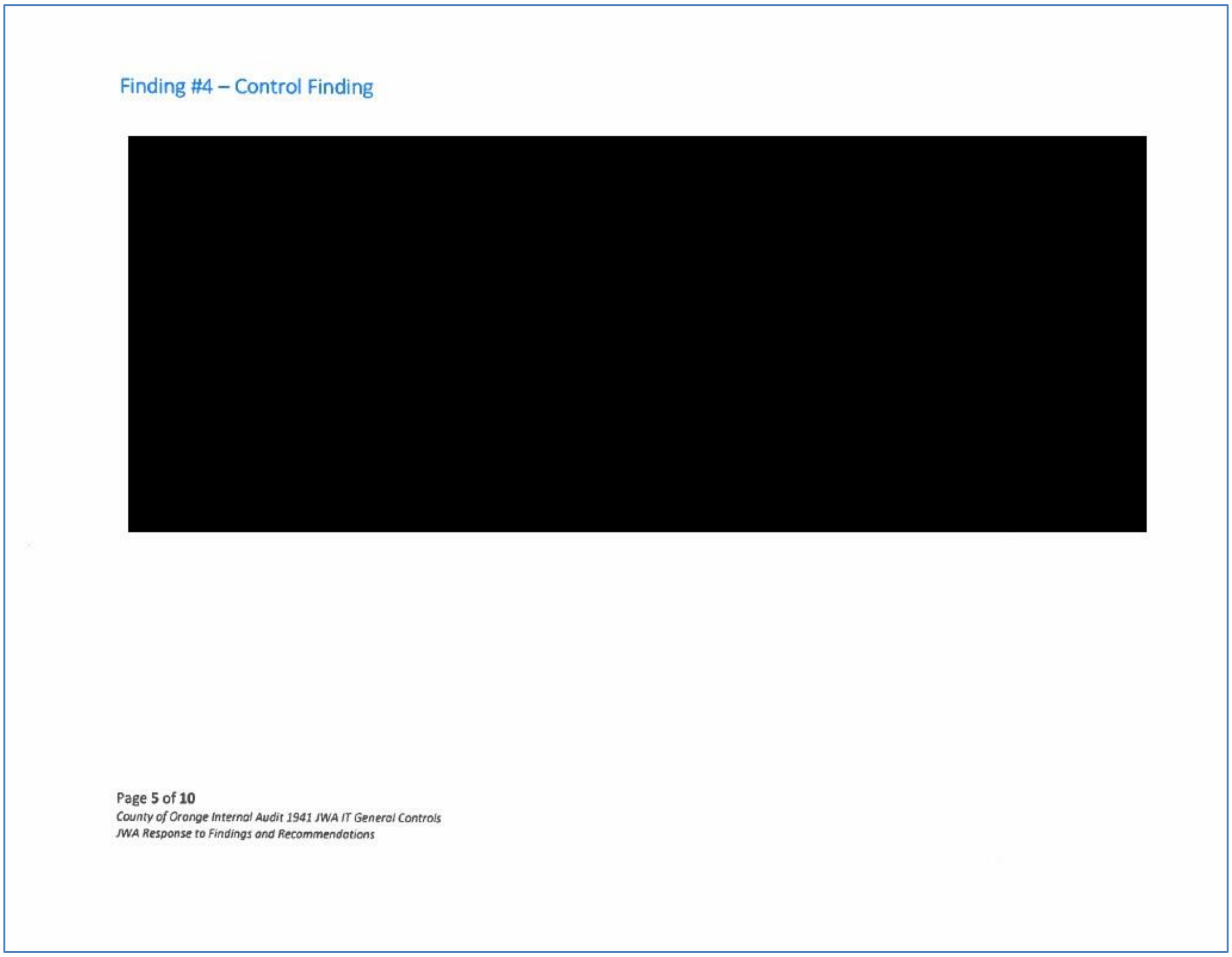
Finding #3 - Significant Control Weakness

[redacted]

Page 4 of 10

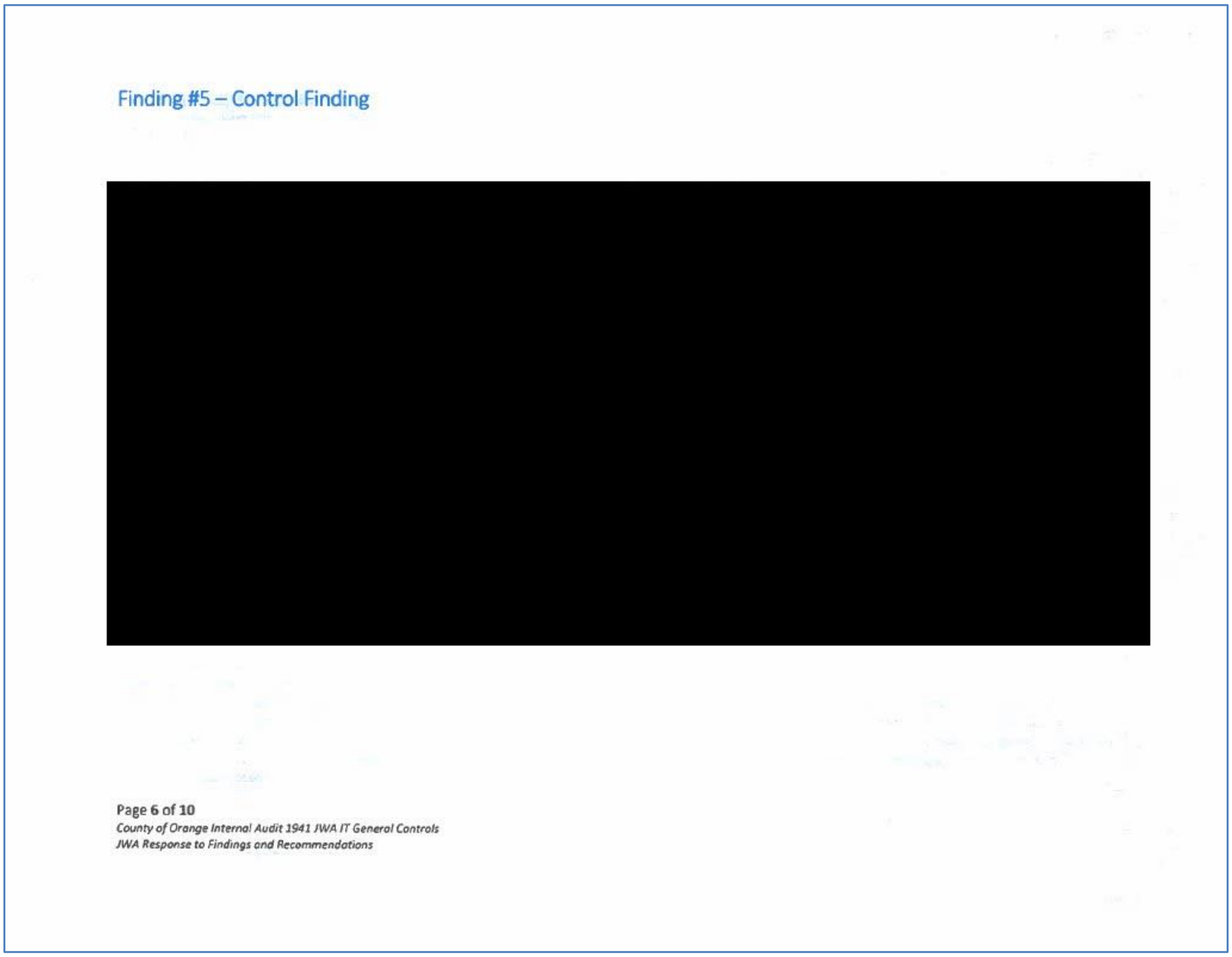
County of Orange Internal Audit 1941 JWA IT General Controls

JWA Response to Findings and Recommendations



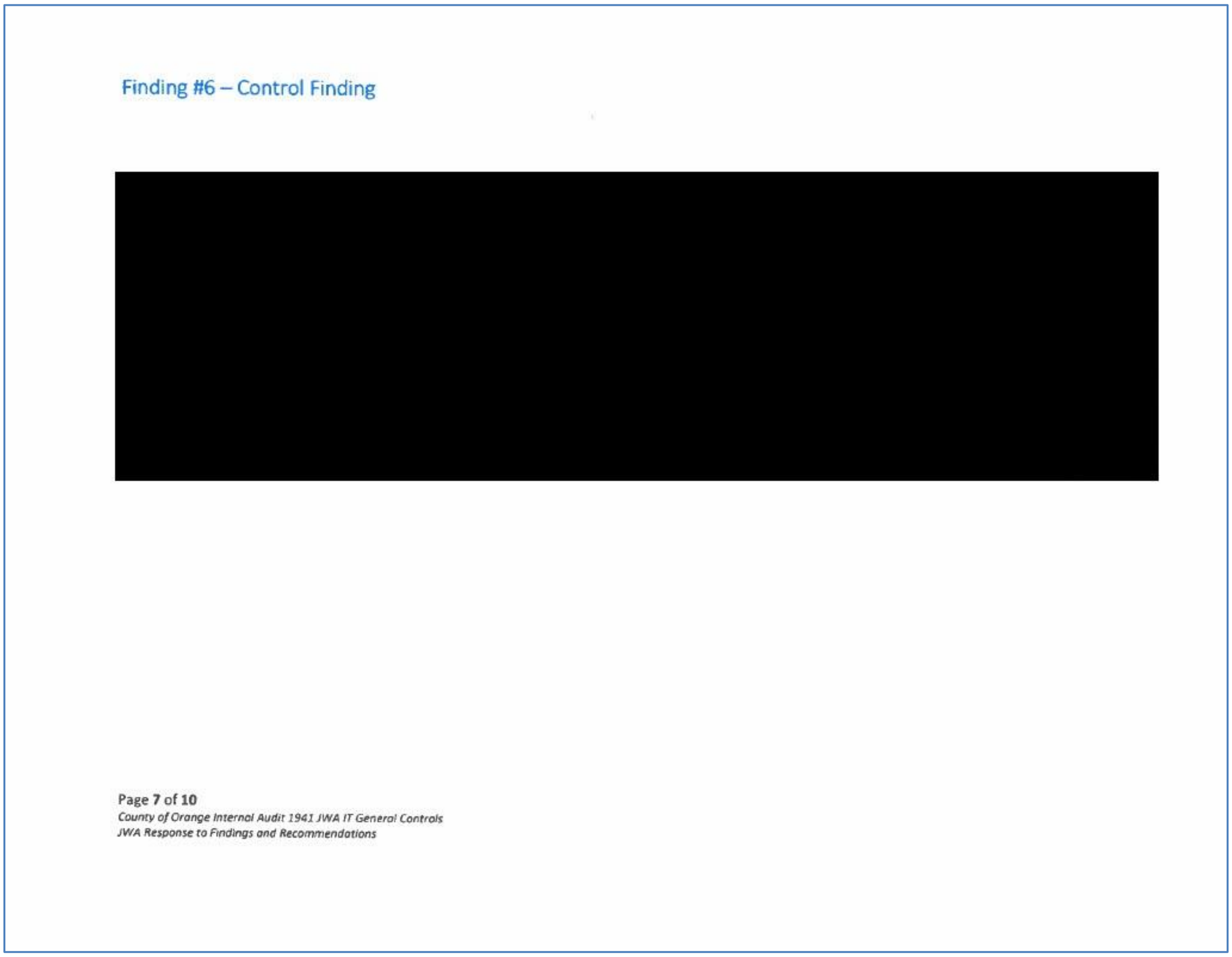
Finding #4 – Control Finding

[redacted]



Finding #5 – Control Finding

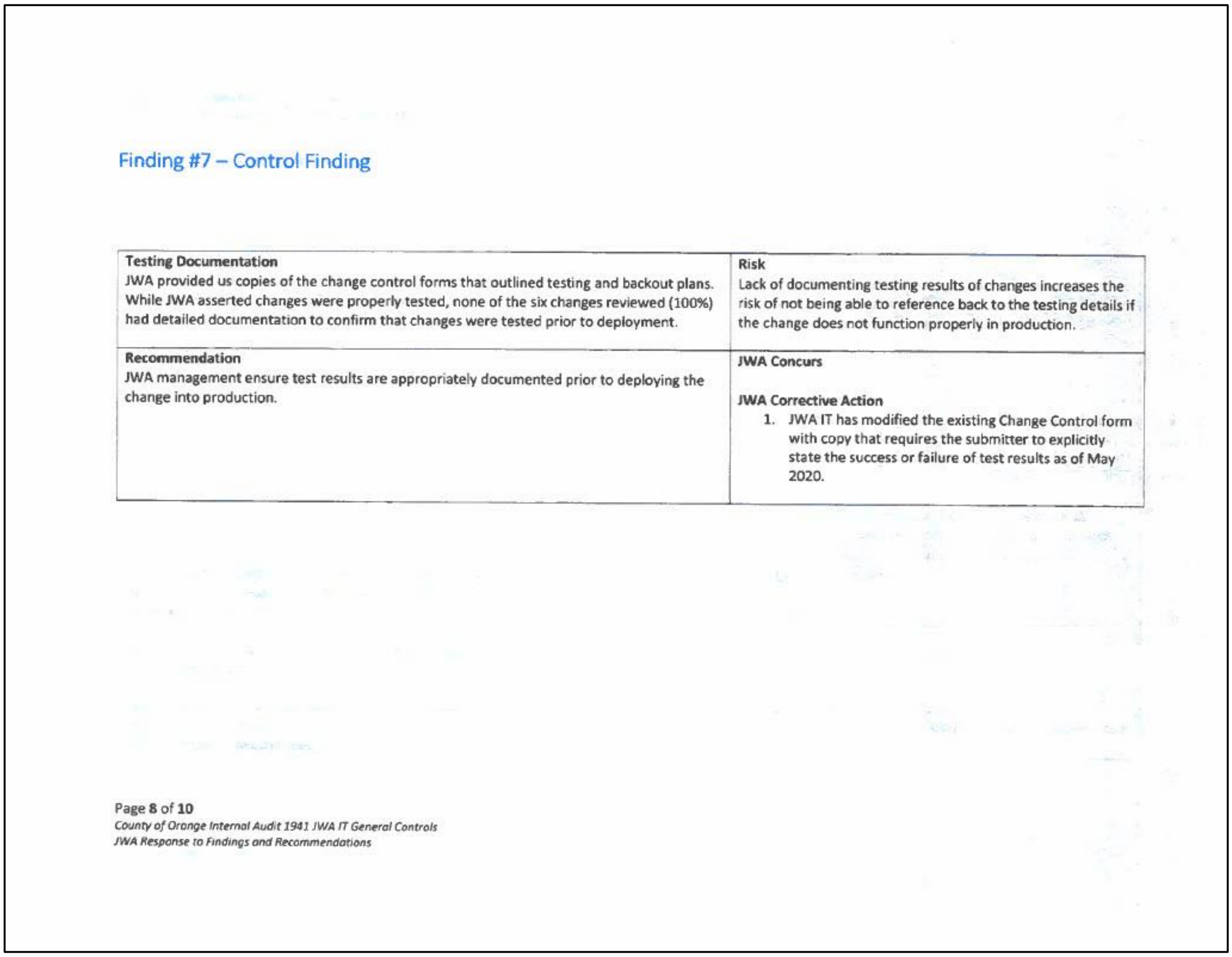
[redacted]



Finding #6 – Control Finding

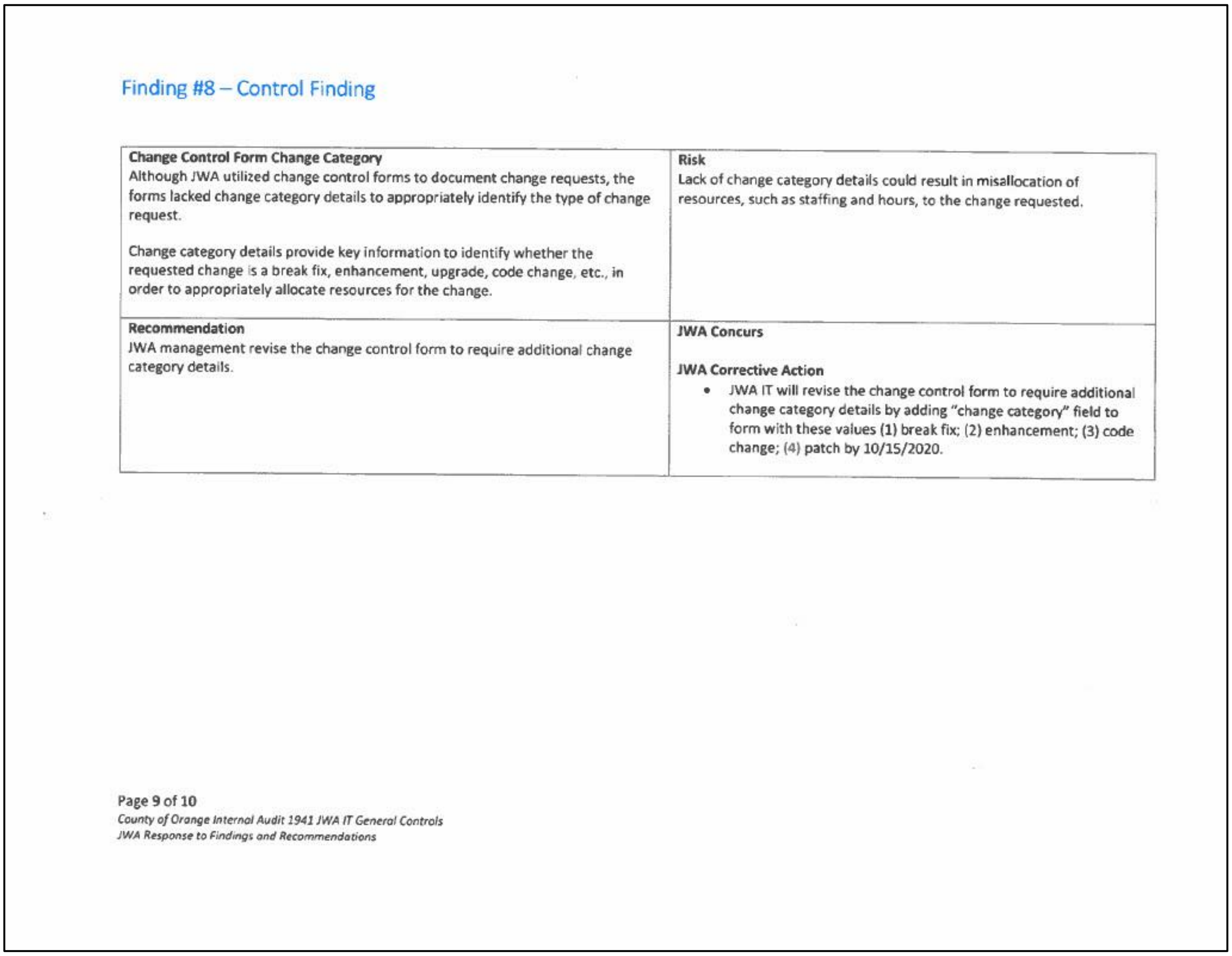
[redacted]

Page 7 of 10
County of Orange Internal Audit 1941 JWA IT General Controls
JWA Response to Findings and Recommendations



Finding #7 – Control Finding

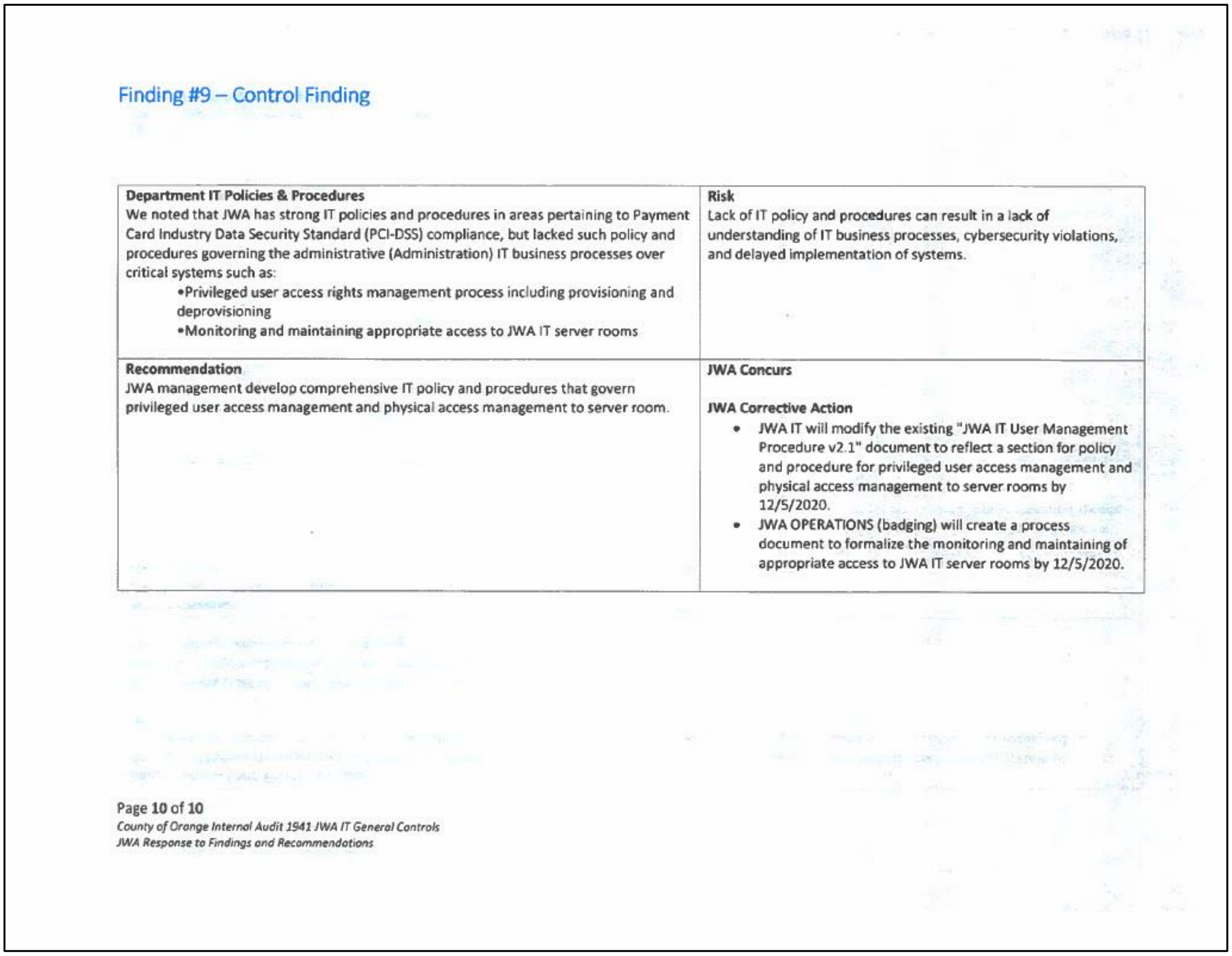
Testing Documentation JWA provided us copies of the change control forms that outlined testing and backout plans. While JWA asserted changes were properly tested, none of the six changes reviewed (100%) had detailed documentation to confirm that changes were tested prior to deployment.	**Risk** Lack of documenting testing results of changes increases the risk of not being able to reference back to the testing details if the change does not function properly in production.
Recommendation JWA management ensure test results are appropriately documented prior to deploying the change into production.	**JWA Concurs** **JWA Corrective Action** 1. JWA IT has modified the existing Change Control form with copy that requires the submitter to explicitly state the success or failure of test results as of May 2020.



Finding #8 – Control Finding

Change Control Form Change Category Although JWA utilized change control forms to document change requests, the forms lacked change category details to appropriately identify the type of change request. Change category details provide key information to identify whether the requested change is a break fix, enhancement, upgrade, code change, etc., in order to appropriately allocate resources for the change.	**Risk** Lack of change category details could result in misallocation of resources, such as staffing and hours, to the change requested.
Recommendation JWA management revise the change control form to require additional change category details.	**JWA Concurs** **JWA Corrective Action** • JWA IT will revise the change control form to require additional change category details by adding "change category" field to form with these values (1) break fix; (2) enhancement; (3) code change; (4) patch by 10/15/2020.

Page 9 of 10
County of Orange Internal Audit 1941 JWA IT General Controls
JWA Response to Findings and Recommendations



Finding #9 – Control Finding

Department IT Policies & Procedures We noted that JWA has strong IT policies and procedures in areas pertaining to Payment Card Industry Data Security Standard (PCI-DSS) compliance, but lacked such policy and procedures governing the administrative (Administration) IT business processes over critical systems such as: •Privileged user access rights management process including provisioning and deprovisioning •Monitoring and maintaining appropriate access to JWA IT server rooms	**Risk** Lack of IT policy and procedures can result in a lack of understanding of IT business processes, cybersecurity violations, and delayed implementation of systems.
Recommendation JWA management develop comprehensive IT policy and procedures that govern privileged user access management and physical access management to server room.	**JWA Concurs** **JWA Corrective Action** • JWA IT will modify the existing "JWA IT User Management Procedure v2.1" document to reflect a section for policy and procedure for privileged user access management and physical access management to server rooms by 12/5/2020. • JWA OPERATIONS (badging) will create a process document to formalize the monitoring and maintaining of appropriate access to JWA IT server rooms by 12/5/2020.