County of San Diego

Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

IT – DISASTER RECOVERY AUDIT

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Khang Nguyen, CISA
Auditor II: Jenny Chen

Report No. A13-008

August • 2014

Intentionally Left Blank

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF AUDITS & ADVISORY SERVICES
5530 OVERLAND AVENUE, SUITE 330, SAN DIEGO, CA 92123-1261
Phone: (858) 495-5991

JUAN R. PEREZ
CHIEF OF AUDITS

August 7, 2014

TO: Mikel Haas, Chief Information Officer
County Technology Office

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: IT – DISASTER RECOVERY AUDIT

Enclosed is our report on the IT - Disaster Recovery Audit. We have reviewed your response to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Franco Lopez at (858) 505-6436.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:FDL:aps

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Brian M. Hagerty, Group Finance Director, Finance and General Government Group
Andrew McDonald, Group IT Manager, Finance and General Government Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of Information Technology (IT) Disaster Recovery (DR). The objective of the audit was to provide reasonable assurance that the management control framework in place to support disaster preparedness for information technology systems is adequate and effective.

Background

The County of San Diego (County) *Information Technology and Telecommunications Service Agreement* (IT Agreement) signed in April 2011 assigns Hewlett Packard Enterprise Services (HP) responsibility for providing disaster recovery management services to the County.

HP prepared the *CoSD-T407 County of San Diego Disaster Recovery Management Plan* (DR Plan) dated December 15, 2011 and provided the DR Plan to the County Technology Office (CTO) for review and approval. This plan defines the recovery strategy, high-level procedures necessary to recover the County's IT technical environments at HP and outlines the roles and responsibilities assigned to HP and the County to ensure rapid recovery of the County's IT environment.

HP maintains critical County application portfolio information in a centralized database called Apps Manager that is the system of record to support IT DR planning and recovery. County departments assign priority classifications to applications in Apps Manager based on criticality and time sensitivity. The application priority determines the recovery time objective (RTO)[1] and recovery point objective (RPO)[2] for each application as follows:

- Priority 1 (P1) applications affect Life, Safety and/or Health and must be recovered within 48 hours following a disaster.
- Priority 2 (P2) applications are Mission Critical affecting critical services provided to other County departments and/or the public and must be recovered within 72 hours following a disaster.
- Priority 3-5 (P3-P5) applications are recovered within "best effort".
- Priority 1 and 2 applications must have an RPO (restored data) no older than 28 hours prior to the disaster.

Audit Scope & Limitations

The scope of the audit focused on evaluating whether key controls are designed and operating effectively to support disaster preparedness for information technology systems at the County as of August 2013.

[1] Recovery Time Objective (RTO) is the maximum tolerable length of time that a business process can be down after a disaster.

[2] Recovery Point Objective (RPO) is the maximum tolerable period in which data might be lost from an IT service due to a major event

The audit was limited to testing DR controls and processes covered in the IT Agreement Schedule 4.3 Section 7.8 Disaster Recovery Management Services. This review focused on the primary HP managed data centers in Tulsa, OK and Plano, TX and the AT&T Point of Presence (POP) data center in San Diego.

OAAS also based their assessment on recommended DR controls, and compliance with standards and guidelines from the following:

- IT Governance Institute's *Control Objectives for Information and related Technology 5 (COBIT 5)*.
- National Institute of Standards and Technology (NIST) *Contingency Planning Guide for Federal Information Systems Special Publication 800-34 Rev.1.*

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

Methodology

OAAS performed the audit using the following methods:

- Interviewed County and HP stakeholders.
- Reviewed industry frameworks and best practices guidance (COBIT 5; NIST 800-34).
- Reviewed the County's DR Plan and the IT Agreement Schedule 4.3 – Operational Services to understand County policies, requirements, and processes.
- Assessed the risks to achieving key DR control objectives independently and with management.
- Identified, reviewed, and tested DR controls for design and operating effectiveness to verify that:
  - Organizational oversight and governance is adequate.
  - The HP Apps Manager and Application Run Books[3] are complete and accurate and provide information needed to recover critical applications for business continuity.
  - The DR Plan sufficiently documents plan details, recovery procedures, communications/network environment, hardware

[3] As outlined in the CoSD-T407 DR Plan, Application Run Books serve as an application's full operations support manual. Run Book's outline all operational and physical requirements in the application environment that are needed to meet the goals of the Application services agreements, including hardware, software and configuration. The Run Books stand to support the operations of the environment in the event that an emergency occurs.

configuration, software applications and supporting platforms, data recovery, facilities, staff, and third-party vendors.

- The DR Plan is distributed to key stakeholders and updated regularly.

- The DR Plan testing and training is administered annually, test results are reviewed and approved by County management, and corrective action is implemented in a timely manner according to the IT Agreement Schedule 4.3.

AUDIT RESULTS

Summary

The management control framework to support disaster preparedness for information technology systems needs improvement. Opportunities for improvement were identified in areas related to:

- Compliance with DR standards and County requirements.
- IT vendor DR risk management.
- DR system of record.

To strengthen current controls and improve the effectiveness of DR controls and processes, OAAS presents the following findings and recommendations.

Finding I: **Compliance with DR Standards and County Requirements Needs Improvement**

A review of the management control framework in place to support DR identified issues related to compliance with DR standards and County requirements as described below.

- **DR Plan for the AT&T POP is Not Fully Completed.** The DR Plan provided by HP to the County on May 13, 2013 does not include recovery of the AT&T POP data center. At the time of the audit, a plan to create redundancy for the AT&T POP was in progress, but not fully completed.

  Since 2008, the County and HP have been researching a feasible DR solution for the AT&T POP. The IT contract transition from Northrup Grumman to HP in April 2011 further delayed the remediation.

  Lack of a complete and tested DR Plan for the AT&T POP increases the risk of loss of network connectivity if a disruptive event at the AT&T POP occurs, potentially resulting in disruption of network communications and preventing County end-users from accessing the network and required information and applications.

- **Inconsistent DR Plan Approval.** County approval of the DR Plan is not consistently retained. The CTO did not retain the conditional

acceptance email sent to HP evidencing their review and approval of the December 15, 2011 DR Plan.

COBIT 5 DSS04.03 states that executive business approval of the DR Plan should be obtained.

- **Undefined DR Test Plan.** HP has not developed a DR test plan or performed a comprehensive test of the County DR Plan. The CTO sent a request to HP on April 10, 2013 to provide a DR test plan initiating this process; however, at the time of the audit, there was no estimated time of completion.

  HP performed an application recovery exercise from backup media for two County applications on December 5, 2011. One of the applications tested, JCATS, is not a P1/P2 application. The County was not involved in the recovery exercise and there was no evidence that test results were reported to or approved by County management.

  Per the IT Agreement Schedule 4.3, HP is responsible for annually producing and submitting a DR test plan, performing DR testing, submitting DR test results, and performing corrective action identified during testing. The County is responsible for annually reviewing and approving the DR test plan and test results, and following-up to ensure that all corrective action is performed. Per the County's DR Plan, this process should be performed at regular intervals not to exceed 12 months. Also, periodic testing of recovery from backup media is an ongoing critical deliverable in the IT Agreement.

  All elements of the DR Plan need to be tested periodically to ensure that gaps in the plan or issues resulting from the test can be identified and corrected in a timely manner. Failure to test all elements of the DR Plan can mean that disaster recovery arrangements on which the County places reliance may not be recovered timely or completely.

- **Undefined DR Training Plan.** DR Plan training has not been administered to key HP and County stakeholders involved in the IT recovery process. Per the County's DR Plan, each framework leader is responsible for reviewing the recovery plans with their employees on a regular basis. Training should be conducted so that members of the application and infrastructure teams can execute the plans if necessary.

  Without periodic DR training, recovery personnel may lack preparation to quickly execute recovery procedures in a disaster situation.

Recommendation: To improve compliance with DR standards and County requirements, the CTO should work with HP to:

1. Complete an approved and tested DR Plan for the AT&T POP.

2. Ensure the County DR Plan approval process is formalized and documentation is adequately retained.

3. To ensure DR readiness and effectiveness, DR testing should be in place to test all elements of system recovery as set out in the IT Agreement and DR training administered regularly, as follows:

   a. Establish a timeline for developing a DR Test Plan and at a minimum perform annual testing to ensure successful coordination and execution of DR procedures among key stakeholders.

   b. Review and approve DR test results to ensure objectives were adequately met. If not met, implement corrective actions in a timely manner and update the DR Plan and source documents.

   c. Perform periodic application recovery from backup media for qualifying P1/P2 applications. Involve the County in the exercise during the application selection process and the review and approval of test results.

   d. Develop and administer mandatory annual DR training to all County and HP personnel who will be directly involved in and responsible for executing the DR Plan.

Finding II: **HP Apps Manager and Application Run Books are Not Complete and Accurate**

DR related information documented in Apps Manager and Application Run Books maintained by HP are not complete or accurate as described below.

- **Apps Manager.** OAAS tested the completeness and accuracy of critical information maintained in Apps Manager for 92 P1/P2 applications supported by HP.
  - Three P1/P2 applications (PA2468, PA2237 and PA1058) had missing or inappropriate priorities. PA2468 is a P2 dependency application but is assigned an 'UNK' priority and the remaining two applications have no assigned priority.

  - Of 92 P1/P2 applications, 11 did not have critical information such as security classification, application platform, operating system, database platform or vendor documented.

- **Application Run Books.** OAAS sampled 10 of the 92 (11%) P1/P2 servers listed on HP's Application Server Report and obtained

Application Run Books for each server. Of the 10 Run Books, 4 (40%) did not document the production server sampled.

Per the CTO and HP, Apps Manager and Application Run Books are the systems of record containing County application system configurations, calling trees, dependencies and priority classification. To facilitate successful DR, these documents should be complete and accurate. The application priority rating determines the recovery priority requirements as outlined in the IT Agreement Schedule 4.3 and the DR Plan.

Incomplete or inaccurate source information required for DR may adversely impact the County's ability to prepare for and perform essential DR activities.

The CTO indicated that the application information was never properly collected and recorded in Apps Manager and the Application Run Books were not up-to-date.

Recommendation: To support the effectiveness of the DR Plan, the CTO should work with HP to ensure that critical application information needed for recovery is accurately and completely recorded in Apps Manager and updated in the Run Books.

DEPARTMENT'S RESPONSE

County of San Diego

MIKEL HAAS
CHIEF INFORMATION OFFICER
(619) 531-5570

COUNTY TECHNOLOGY OFFICE
1600 PACIFIC HIGHWAY ROOM 306F, SAN DIEGO CA 92101
www.sdcounty.ca.gov/cto

SUSAN GREEN
ASSISTANT CHIEF INFORMATION OFFICER
(619) 515-4337

August 6, 2014

Ref: 14-IA-366

RECEIVED

AUG 07 2014

OFFICE OF AUDITS &
ADVISORY SERVICES

TO: Juan Perez
Chief of Audits

FROM: Mikel Haas, CIO
County Technology Office

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: IT – DISASTER RECOVERY AUDIT

Finding I: Compliance with DR Standards and County Requirements Needs Improvement

OAAS Recommendation: To improve compliance with DR standards and County requirements, the CTO should work with HP to:

1. Complete an approved and tested DR Plan for the AT&T POP.

   Action Completed: The CTO has engaged HP through the Contracts department to deliver an approved updated DR Plan, to include the AT&T Alternate POP location, through the Critical Milestones Process. The AT&T Alternate POP location was put in place and tested in September of 2013. There is a second phase to implementing the Alternate POP location to finalize the redundant connections to the HP Data Centers that will complete the AT&T POP portion of the DR Plan.

   Planned Completion Date: The Plan was delivered and approved in June 2014 via the Critical Milestones. The second phase of the AT&T Alternate POP is being defined under a project currently in flight estimated to be complete by Dec 2014, and the DR Plan will be updated with the new data and delivered for formal approval by the CTO immediately following.

   Contact Information for Implementation: Joseph Schlientz – Operations and Infrastructure Service Manager

2 Ensure the County DR Plan approval process is formalized and documentation is adequately retained.

Action Completed: The DR Plan is a formal deliverable within the contractual Schedule 5 Report Process. It is identified as Report # 73 and is scheduled to be delivered and approved annually. This documentation is located and archived within the ITSC website, and within the Contracts Office within the CTO.

Planned Completion Date: Done/ Ongoing

Contact Information for Implementation: Dorothy Gardner – Contracts Manager

3 To ensure DR readiness and effectiveness, DR testing should be in place to test all elements of system recovery as set out in the IT Agreement and DR Training administered regularly, as follows

a. Establish a timeline for developing a DR Test Plan and at a minimum perform annual testing to ensure successful coordination and execution of DR procedures among key stakeholders.
b. Review and approve DR test results to ensure objectives were adequately met. If not met, implement corrective actions in a timely manner and update the DR Plan and source documents.
c. Perform periodic application recovery from backup media for qualifying P1/P2 applications. Involve the County in the exercise during the application selection process and the review and approval of the test results.
d. Develop and administer mandatory annual DR Training to all County and HP personnel who will be directly involved in and responsible for executing the DR Plan.

Action Completed: The CTO has engaged HP through a formal Contracts letter notifying them of the immediate need for an acceptable DR Test Plan to be delivered for approval. The DR Test Plan is formally identified within the contractual Schedule 5 Reports Process as Report # 74, and is due for delivery and approval annually. The DR Test Plan will include all aspects of recovery and failover for identified P1/P2 applications and their dependencies, and would also include an area identified to perform Training for all stakeholders involved on an annual basis. The Schedule 5 Report Process also includes a Report # 75 The DR Test Plan Results Report, which is due annually as well, and would include all results from the testing of each aspect of the DR Plan as well as actions required to address any inadequacies found during the Test exercises.

Planned Completion Date: The CTO has requested this be completed as soon as possible via Contract letter

Contact Information for Implementation: Joseph Schlientz – Operations and Infrastructure Service Manager

Finding II: HP Apps Manager and Applications Run Books are not Complete and Accurate

OAAS Recommendation: To support the effectiveness of the DR Plan, the CTO should work with HP to ensure that the critical application information needed for recovery is accurately and completely recorded in the Apps Manager and updated in the Run Books.

Action Plan: Run Books today are standalone documents that contain information that is also stored in other places. That is being eliminated and the Run Books will be generated from Apps Manager as a report. This will solve the problem with keeping the Run Book data up to date.

For Apps Manager data quality, HP is implementing a Quality Assurance step in their Project Closure Checklist process to check Apps Manager for accuracy.

Planned Completion Date: Run Book generation from Apps Manager will be completed by December 31, 2014. The Quality Assurance process for Apps Manager will be implemented by August 31, 2014.

Contact Information for Implementation: Jim Leonard – Applications Service Manager

If you have any questions, please contact Joe Schlientz at (619) 531-4812 or myself at (619) 685-2397.

Regards,

Mikel Haas
Chief Information Officer

CC: Susan Green