County of Ventura
AUDITOR-CONTROLLER
MEMORANDUM

To: Brian Ganley, Chief Information Officer,
Information Technology Services Department

Date: May 2, 2019

From: Jeffery S. Burgh

Subject: **AUDIT OF INFORMATION TECHNOLOGY SERVICES DEPARTMENT DISASTER RECOVERY PLANS**

We have completed our audit of the Information Technology Services Department ("ITSD") Disaster Recovery Plans ("DRPs"). Each County department is responsible for developing and maintaining DRPs for the department's own mission critical County IT systems, and our audit focused on the DRPs that were the responsibility of ITSD. Our overall audit objective was to determine whether ITSD's DRPs were adequately documented and approved, subject to periodic reliability testing, and supported by vendor agreements. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* promulgated by The Institute of Internal Auditors. Our findings are summarized below with details provided in the attached report.

EXECUTIVE SUMMARY

Overall, we found that ITSD's DRP program was in need of improvement to ensure continuity of vital County services in the event of a disaster. While ITSD has started to strengthen its DRP program by assigning responsibility to a new Deputy Chief Information Officer and exploring methods for centralizing the DRP process, our audit disclosed areas where action was needed to ensure timely restoration of information technology systems. Specifically, we found that:

- Although a Countywide disaster recovery policy exists, ITSD had not documented clearly defined, department-specific DRP program procedures, which likely contributed to most of the subsequent findings in this report.

- ITSD did not always maintain DRPs through regular updates, testing, and training.

- DRPs did not always contain all information needed to support successful restoration of mission critical information technology systems within required timelines.

- Most of the County's redundant sites are located close to the main data center; therefore, a single disaster could theoretically disable multiple sites simultaneously.

- As noted in our prior 2015 audit, *Audit of the Information Technology Department's Role in Information Technology Governance*, the Countywide disaster recovery policy has not been updated in over 10 years.

- Contracts with outside vendors for disaster-related services and equipment existed but did not always contain all recommended clauses to protect the County’s interests.

ITSD management initiated corrective action to address our findings. Corrective action is planned to be completed by June 30, 2020.

We appreciate the cooperation and assistance extended by you and your staff during this audit.

Attachment

cc: Honorable Steve Bennett, Chair, Board of Supervisors
Honorable Kelly Long, Vice Chair, Board of Supervisors
Honorable Linda Parks, Board of Supervisors
Honorable Robert O. Huber, Board of Supervisors
Honorable John C. Zaragoza, Board of Supervisors
Michael Powers, County Executive Officer

County of Ventura

Office of the Auditor-Controller

AUDIT OF INFORMATION TECHNOLOGY SERVICES DEPARTMENT
DISASTER RECOVERY PLANS

May 2, 2019

Jeffery S. Burgh
Auditor-Controller

AUDIT OF INFORMATION TECHNOLOGY SERVICES DEPARTMENT
DISASTER RECOVERY PLANS

TABLE OF CONTENTS

Page

AUDIT OF INFORMATION TECHNOLOGY SERVICES DEPARTMENT
DISASTER RECOVERY PLANS

BACKGROUND

County Administrative Policy No. Chapter V-3, *Information Technology Strategy*, states: "The County cannot operate effectively without computer-based information systems. Basic County services such as justice, public safety, health, welfare, revenue collection, and others depend on these systems." To ensure those technologies are available in the event of a disaster, plans must be made to fully restore those technologies and minimize operational downtime.

Key elements of a disaster recovery plan ("DRP") program include:

- developing a DRP program policy and procedures (e.g., establishing roles and responsibilities, program scope and objectives, resource and training requirements, maintenance schedule, etc.);
- identifying mission critical County information technology ("IT") systems and the priorities for restoring those systems;
- developing detailed plans for restoring critical systems within required timelines;
- providing periodic training to individuals responsible for executing DRPs; and
- regularly testing and updating the plans to ensure the DRPs will function as intended in the event of a disaster.

Each County department is responsible for developing and maintaining DRPs for the department's own mission critical County IT systems. While the Information Technology Services Department ("ITSD") is responsible for developing DRPs for ITSD's own internal systems and certain key Countywide IT infrastructure, DRPs for other County IT systems are the responsibility of the department that owns the respective business process.

SCOPE

Our audit focused on ITSD and the DRPs that were associated with ITSD's Continuity of Operations Plan ("COOP") at the time of our audit during fiscal year 2017-18 (collectively, "ITSD's DRPs"). This audit did not review DRPs that are the responsibility of departments other than ITSD, or the overall system of DRPs for the County as a whole. Our audit also did not include review of COOPs or whether ITSD's DRPs addressed all of ITSD's mission critical County IT systems. This audit does not provide an opinion on the ability of ITSD's DRPs to restore operations in the event of a disaster.

Our overall objective was to determine whether ITSD's DRPs were adequately documented and approved, subject to periodic reliability testing, and supported by vendor agreements. Specifically, we:

- verified that DRPs were based on an up-to-date, comprehensive risk assessment;
- verified that ITSD had maintained DRPs through regular updates, testing, and training;
- verified that DRPs contained sufficient information to enable restoration of mission critical County IT systems within required timelines;
- evaluated the reasonableness of redundant site locations and verified incorporation into the DRPs; and

- determined whether vendor agreements supported DRP restoration efforts and identified liability responsibilities if a vendor failed to provide the services outlined within the agreement.

In performing our audit, we referenced requirements outlined in the County's *Information Technology Disaster Recovery Policy and Standards*, as well as County Administrative Policy Manual Chapter V, *Information Management*. In addition, we referenced leading practices from standards and guidance published by the following entities:

- National Fire Protection Association ("NFPA")
- National Institute of Standards and Technology ("NIST")

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* promulgated by The Institute of Internal Auditors.

FINDINGS

Overall, we found that ITSD's DRP program was in need of improvement to ensure continuity of vital County services in the event of a disaster. While ITSD has started to strengthen its DRP program by assigning responsibility to a new Deputy Chief Information Officer and exploring methods for centralizing the DRP process, our audit disclosed areas where action was needed to ensure timely restoration of IT systems.

We found that, although a Countywide disaster recovery policy exists, ITSD had not documented clearly defined, department-specific DRP program procedures, which likely contributed to most of the subsequent findings in this report. We also found that ITSD's DRPs did not appear to be based on a comprehensive, recently-updated risk assessment.

ITSD did not always maintain DRPs through regular updates, testing, and training. For example, 8 of 10 sampled DRPs had not been updated within the last 5 years, with one DRP that had not been updated in more than 10 years. ITSD's DRPs also did not have evidence of management approval, which would provide formal authorization for the plans and provide recovery team members with the authority and responsibility to execute the plans. Further, paper or other off-line copies of DRPs were not actively maintained and readily accessible for recovery teams to use in case cloud or network copies are inaccessible.

DRPs did not always contain all information needed to support successful restoration of mission critical County IT systems within required timelines. For example, all 10 of the sampled DRPs lacked one or more items, such as detailed steps for restoring systems and alternative measures that can be used if the primary restoration method fails.

We found that DRPs did not always assign specific roles and responsibilities to recovery team members, and contact information for team members was not always included or up-to-date. For example, of 59 DRP team members we reviewed, 33 (56%) either had outdated contact information or did not have any contact information (e.g., a phone number) listed in the DRP.

We found that all but one of the County's redundant sites were located within 30 miles of the primary data center, which increases the chances that a single disaster (e.g., an earthquake) could disable multiple sites at once.

As noted in our prior 2015 audit report, *Audit of the Information Technology Services Department's Role in Information Technology Governance*, Countywide IT policies were not always reviewed and updated on a regular basis. During our current audit, we found that the County's *Information Technology Disaster Recovery Policy and Standards* had not been updated in over 10 years.

Finally, we found that ITSD's contracts with outside vendors providing disaster recovery-related services and equipment existed but did not always contain all recommended clauses to protect the County's interests. For example, vendor agreements did not always specify how quickly goods and services were to be delivered in the event of a disaster, or contain penalty clauses for vendor non-performance.

Following are details of the areas where improvements were needed. ITSD management initiated corrective action during the audit as noted.

1. **Documented Department DRP Program Procedures.** Although a Countywide disaster recovery policy exists, ITSD had not documented clearly defined, department-specific DRP program procedures as of the time of our field work. As noted in NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Section CP-1: "The organization develops, documents, and disseminates…procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls…." Leading practice guides published by NFPA and NIST recommend that organizations develop management-approved DRP program documentation that incorporates some or all of the following elements:

   - Roles and responsibilities
   - Program scope, goals, performance, objectives, and metrics for program evaluation
   - Relationship and coordination between DRPs and associated planning documents (e.g., COOP, business impact analysis, etc.)
   - Resource requirements
   - Training requirements
   - Exercise and testing schedules
   - Plan maintenance schedule
   - Records management
   - Change management

   We noted that the lack of documented procedures likely contributed to most of the subsequent findings in this report.

   Recommendation. ITSD should develop, obtain management approval for, and implement department-specific DRP program procedures including items such as the ones listed above.

   Management Action. ITSD management stated:

   "IT Services agrees with this finding.

   "The existing Information Technology Disaster Recovery Policy and Standards document is published on the County's website http://vcportal.ventura.org/VCWEB/policies/docs/IT_Disaster_Recovery.pdf).

"Additionally, the County's 'Steps to an IT Disaster Recovery Policy and Standards' document outlines the elements needed to successfully document a suitable disaster recovery plan.

"It is agreed that the documents should be updated. IT Services is recruiting a Chief Information Security Officer and one of their duties will be to update the existing documents.

"We will also develop and implement department-specific DRP program procedures.

"Estimated Completion Date: June 30, 2020"

2. **Risk Assessment.** ITSD's DRPs did not appear to be based on a comprehensive, recently-updated risk assessment. In order to select appropriate disaster recovery responses and formulate a DRP, organizations need several pieces of information from a risk assessment or business impact analysis, including:

- An up-to-date list of critical IT systems
- Restoration priorities for those systems (i.e., which systems need to be restored first)
- Recovery Time Objective ("RTO") (i.e., the period of time within which a system must be recovered after an outage)
- Recovery Point Objective ("RPO") (i.e., the maximum amount of data loss the organization can sustain during an event)

While ITSD has a list of critical IT systems and restoration priorities generated through the COOP process, ITSD's COOP had not been updated in over a year at the time of our field work, and did not incorporate all of the items listed above. Without an up-to-date list of all critical systems, RTOs, and RPOs, ITSD would not be able to ensure that sufficient DRP documentation is available to restore all needed functionality within required timelines.

Recommendation. ITSD should ensure DRPs are based on regularly-updated (e.g., annual) risk assessments/business impact analyses that incorporate the items listed above.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services will update the departmental COOP plan which will identify the critical systems utilized by IT Services and serve as our risk assessment. The COOP recognizes that the County has hundreds of systems with priorities assigned. The extent and type of each specific disaster scenario will determine and impact the RTO/RPO for each system.

"It is agreed that the list of critical systems should be updated so that documentation can be verified. It however should be noted and acknowledged that an RTO/RPO is an objective for recovery and is not guaranteed to be met given the circumstances of each specific disaster.

"Estimated Completion Date: December 31, 2019"

3. **DRP Maintenance.** ITSD did not always maintain DRPs through regular updates, testing, and training. The "Testing Requirements Schedule" contained in the majority of DRPs in our sample states: "The IT Disaster Recovery Project Manager shall manage the IT Services Disaster Recovery Plan Maintenance & Testing Schedule, to insure reviews and testing exercises are properly tracked, scheduled and performed." In addition, ITSD did not always ensure that DRPs had documented management approvals and did not maintain readily accessible paper or other off-line copies of DRPs.

   A. **DRP Updates.** ITSD's DRPs were not always updated on a regular basis. Out of 10 DRPs that we reviewed, 8 (80%) had not been updated in more than 5 years, including one DRP that had not been updated in more than 10 years. The "Maintenance Requirements Schedule" contained in the majority of DRPs in our sample suggested that DRPs are to be updated annually by stating: "This plan shall be reviewed, updated, approved and distributed on the following intervals: 1) During the annual tabletop test for procedure validation and accuracy; 2) After the Annual Disaster Recovery Test to address any issue encountered". Without regular updates to reflect changes in the system restoration process, ITSD might not be able to restore mission critical IT systems in a timely manner in the event of a disaster.

      Recommendation. ITSD should establish and implement policies and procedures to ensure that DRPs are reviewed and updated on a regular basis (e.g., at least annually, with additional updates if configuration changes significantly impact DRPs).

      Management Action. ITSD management stated:

      "IT Services agrees with this finding.

      "IT Services will be purchasing a DR Plan system to document the DR Plan and other necessary information for each critical system. Information in this new system will be updated in accordance with the revised County's Information Technology Disaster Recovery Policy and Standards document.

      "Estimated Completion Date: December 31, 2019"

   B. **Regular, Documented DRP Tests.** ITSD did not always test DRPs to ensure the plans would perform as expected in an emergency. For the one test in which ITSD regularly participates, the results are not documented to provide evidence the test took place and facilitate improvement actions.

      i. **Regular Testing.** ITSD's DRPs were not always tested to ensure that the plans would perform as expected in the event of an emergency. While ITSD participates in a periodic testing of one system, no other ITSD DRPs have been tested within the last 5 years. The "Testing Requirements Schedule" contained in the majority of DRPs in our sample states that DRPs "…shall be tested at least once annually." Insufficient DRP testing may create a gap between restoration expectations and what can realistically be accomplished. Furthermore, testing may allow for identification of process improvements that could result in more efficient use of resources.

Recommendation. ITSD management should establish periodic (e.g., annual) testing of DRPs for all critical systems, including both smaller scale (e.g., tabletop) tests and full simulation tests. Although annual tests may be performed on a smaller scale, full simulation testing should be performed periodically to determine whether DRPs can be used to fully restore critical systems within required timelines. To ensure full system functionality, testing must include business owners or owner representatives who can confirm access and functionality of the affected applications.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services will update the existing policy to reflect periodic testing, along with a log to document those tests. The DR Plan system IT Services will be purchasing has a module for testing and recording results.

"While it may not be feasible to conduct a full test of each of the County's systems every year, a likely approach would be rotating through a subset of each of the critical systems annually for testing, with validation of updated plans occurring annually for all systems that are not being tested in that year.

"Estimated Completion Date: June 30, 2020"

ii. **DRP Test Documentation.** ITSD has not formally documented the results of the system test that is performed on a periodic basis. Historically, results and lessons learned have been discussed over the phone or e-mail. Documenting test results provides a number of benefits, including:

- providing evidence that the test was performed;
- clarifying what was (and was not) tested;
- identifying areas for improvement; and
- allowing for easier tracking and follow-up on planned improvement actions.

Recommendation. ITSD management should formally document DRP test results for all methods by which recovery plans were tested (i.e., tabletop, walk through, simulation). Documented results should also be sent to a designated management authority to coordinate document retention and ensure that follow-up occurs on any lessons learned to reduce inefficiencies during the next test.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services has conducted some DR Testing for some Critical Systems, and while the results have not formally been documented, the process to conduct the test has been documented.

With each test, the testing procedure documented is updated to reflect any necessary changes to the process to ensure the success of the test.

"IT Services will document the results of each test in the upcoming DR planning system, using the system's module for testing and recording results. DR Plans for Critical Systems will be tested and documented in accordance with the updated procedure.

"Estimated Completion Date: June 30, 2020"

C. **Regular Training for Responsible Parties.** Personnel identified as being responsible for carrying out DRPs were not always trained regarding DRP roles and expectations. Of the 16 DRP team members we selected and interviewed, 5 (31%) had not had any recent DRP training. According to the County *Information Technology Disaster Recovery Policy and Standards*, "Each County department or agency shall sufficiently train staff persons within their offices as alternates for key personnel necessary for information system recovery purposes." Lack of training may prevent employees from effectively executing assigned responsibilities during a disaster.

Recommendation. ITSD should ensure that periodic training is provided to personnel responsible for carrying out DRPs regarding roles and responsibilities. The training program should be documented and modified based on results of periodic DRP tests to ensure that future training is more effective.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"It should be noted that recovery for systems involves regular tasks performed by personnel frequently, although those tasks may not be documented in the DR plan, this serves as a form of ongoing training.

"However, during the testing and documentation process that will be updated and performed based on the findings above, staff will be included and trained during that time, which will be documented accordingly.

"Estimated Completion Date: June 30, 2020"

D. **Formal DRP Approval.** None of the 10 sampled DRPs had evidence of document approval by management or authorized personnel as required by the County's *Information Technology Disaster Recovery Policy and Standards*. According to the policy statement, "All mission critical County of Ventura information technology systems must have a Disaster Recovery Plan that is fully documented, approved, and is subject to periodic reliability testing." Documentation of management approval provides formal authorization for the plans and provides recovery team members with the authority and responsibility needed to execute the plans.

Recommendation. ITSD should ensure that management approvals are obtained for each DRP and ensure that each DRP contains a designated section to document those approvals.

Management Action. ITSD management stated:

“IT Services agrees with this finding.

“IT Services will be purchasing a DR Plan system to record the DR Plan (and other necessary information) about each critical system. The system has workflow for the approval process of the DR Plans.

“A procedure will be established identifying the signature authority for approval of the plans.

“Estimated Completion Date: December 31, 2019”

E. **Copies of DRPs.** DRPs were not actively maintained and readily accessible to recovery teams in paper or another format accessible off-line. Based upon discussion with ITSD management and sampled DRP team members, we noted that off-line copies were not kept or no one was aware of the existence of off-line copies. If ITSD stores copies of DRPs either in the cloud or on the County network, and connectivity to those resources is disabled, recovery teams might not be able to access those DRPs. As a result, restoration efforts could be delayed.

Recommendation. ITSD management should distribute DRPs in hard copy (or other appropriate off-line format) to recovery team leaders for instances when DRPs stored in the cloud or on the County network are not accessible. Additionally, policies should be created to reflect requirements for maintaining and securely storing off-line copies of DRPs.

Management Action. ITSD management stated:

“IT Services agrees with this finding.

“IT Services currently stores the DR Plans as PDFs in the cloud, which is accessible either internally within the County network or remotely.

“In addition, IT Services currently stores all the DR Plans (and other Disaster related information) on a laptop that is shipped offsite for safe storage and retrieval when necessary.

“In accordance with the updated procedures discussed in previous findings above, IT Services will include in its training process for staff information regarding the availability of DR Plans in County systems, as well as cloud based systems that would be available remotely, and offline resources such as the laptop that is stored offsite.

“Estimated Completion Date: September 1, 2019”

4. **DRP Contents.** DRPs did not always contain all information needed to support successful restoration of mission critical County IT systems within established operational guidelines. While a Countywide template exists that provides guidance on documenting DRPs, the template had not been updated in over 10 years and ITSD did not use the template for any of the 10 sampled DRPs we reviewed. All 10 of the sampled DRPs lacked the following:

- Detailed restoration steps: Detailed, step-by-step instructions for restoring mission critical County IT systems correctly and timely, including infrastructure information, steps for validating system functionality, and how long each step takes to complete. The instructions should allow for the system to be recovered within the business' operational requirements.

- Alternative measures: Alternative steps that can be used to restore the system if one or more of the originally planned steps fails.

In addition, 9 (90%) of the 10 sampled DRPs were missing the following information:

- Redundant locations: Redundant site information, including instructions; addresses and/or contact information; and documented steps regarding setup and stabilization of each redundant site, including maximum time allotted until operational.

- Redundant methods: Identification of redundant methods (e.g., backup tapes, disks, drives) to restore data.

- Power supplies: Availability of uninterrupted power supplies ("UPS") or generators, or a reference to a document containing this information.

- Recovery of system networks: Outline of the recovery of system networks and infrastructure to establish data communication to critical applications.

Finally, 2 (20%) of the 10 sampled DRPs did not have a revision history to track when updates were made, who made the updates, and a summary of what was updated. Without these important elements, DRPs might not be effective and could result in delays to restoring mission critical County IT systems.

Recommendation. ITSD should utilize a standardized DRP template and update DRP content to include the items listed above.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services will be purchasing a DR Plan system to record the DR Plan (and other necessary information) about each critical system. The system will establish new templates and will contain all the information noted above.

"Estimated Completion Date: December 31, 2019"

5. **DRP Team Roles, Responsibilities, and Contact Information.** Information regarding DRP team members was not always established, complete, and up-to-date.

   A. **DRP Team Roles and Responsibilities.** DRPs did not always specify team members, alternate team members, and/or team member roles and responsibilities for executing DRPs. In our review of a sample of six DRPs, we found that two did not specify any team members, and a third DRP provided a list of names but did not specify each individual's role and responsibilities. Since these DRPs did not contain complete team role assignments, the DRPs also did not contain:

- a "call tree" (i.e., a document that graphically depicts the calling responsibilities and the calling order used to contact DRP team members); or
- instructions for when and where the team members should rendezvous in case of an emergency.

Without assigning specific responsibilities and providing instructions to team members, delays or gaps may occur in executing the DRP.

Recommendation. ITSD should utilize a standard template and update DRPs to establish team members and document associated roles and responsibilities, as well as alternate team members for important roles. The template should include a "call tree" and rendezvous instructions (including a prioritized list of alternate locations) for team members in the DRP.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services currently utilizes cloud based systems to record contact information and standard operating procedures/run books for several systems/processes. Some of this information is currently not included in some DR Plans.

"IT Services will be purchasing a DR Plan system to record the DR Plan as well as contact information for staff and vendors. IT Services will ensure that our staff are trained on the proper use of the DR Plan system and their roles in Disaster Recovery. The DR Plan system contains information to establish team members and document associated roles and responsibilities, as well as alternate team members for important roles.

"Estimated Completion Date: December 31, 2019"

B. **Contact Information.** Contact information for team members responsible for executing DRPs was not always complete and up-to-date. Of the 59 team members reviewed, 2 (3%) did not have any contact information (e.g., telephone numbers) listed within the document, and 31 (53%) had outdated contact information (i.e., team member is no longer part of the recovery process, phone number changed, etc.). Our review disclosed that 11 individuals listed as team members were retired and 2 individuals were deceased at the time of our testing. Such oversight may result in difficulty executing DRPs should a disaster occur.

Recommendation. ITSD should implement a periodic process (e.g., at least annually) to review and update recovery team contact information, including a home and mobile phone number in addition to a work phone number. ITSD should ensure that recovery team information is included within the DRP document.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services currently uses a cloud based system to maintain current contact information including home, mobile, and office numbers for each IT Services employee. The cloud based system is accessible from within the County network and remotely.

"IT Services will be purchasing a DR Plan system that integrates with our cloud based system to record the DR Plan as well as contact information for staff and vendors. IT Services will ensure that our staff are trained on the proper use of the DR Plan system and their roles in Disaster Recovery. IT Services will update the contact information annually.

"Estimated Completion Date: December 31, 2019"

6. **Proximity of Redundant Sites.** In the DRPs we reviewed, all but one of the County's redundant site locations for restoring system operations are within a 30 mile radius of the County's primary data center(s), and thus could be impaired by the same disaster. NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Section CP-7(1) recommends that organizations identify "…an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats." A single disaster (e.g., an earthquake) in Ventura County could result in both the primary and redundant sites being rendered unavailable to execute the DRPs.

   Recommendation. ITSD should conduct a formal evaluation to consider the risk of losing multiple data centers and/or redundant site locations against the costs for relocating redundant sites outside the geographic area of the primary data center(s). The evaluation should be documented, providing either rationale for maintaining the current redundant site locations or proposals for any needed changes. Once completed, the evaluation should be presented to the County Executive Office ("CEO") and the County's IT Committee for support and approval.

   Management Action. ITSD management stated:

   "IT Services agrees with this finding.

   "IT Services currently has contracts with two different vendors to provide Disaster Recovery services. One will provide trailers for the housing of a temporary data center and office space for staff. The other provides for computer equipment. These sites are currently specified within the above mentioned 30-mile radius of the primary data center. IT Services will review these contracts to identify the best possible locations.

   "IT Services also currently sends back ups offsite using a third party. IT Services will review that contract to determine the best possible location.

   "IT Services is also currently evaluating redundant site locations to house our critical systems and the redundant backup solution.

   "Estimated Completion Date: September 1, 2019"

7. **Countywide Disaster Recovery Policy.** The Countywide disaster recovery policy, *Information Technology Disaster Recovery Policy and Standards*, has not been updated in over 10 years. While the CEO is ultimately responsible for creating and enforcing information technology policies, according to County Administrative Policy No. Chapter V-3, *Information Technology Strategy*, ITSD "…has been mandated the responsibility and authority for drafting standards, [and] recommending policies and guidelines…" to the CEO. We previously identified this concern in our prior audit report, *Audit of the Information Technology Services Department's Role in Information Technology Governance*, dated March 30, 2015; however, corrective action has not been completed. Given the rapidly evolving technological landscape, ITSD should ensure that policies are reviewed on a regular (e.g., annual) basis and updated to ensure that departments have reliable guidance for creating DRPs.

   Recommendation. ITSD should update the County disaster recovery policy for CEO approval. ITSD should also develop and follow a schedule for regular (e.g., annual) review and update of the disaster recovery policy. Policy reviews should be documented within a document revision log to track dates of review and changes made to the document.

   Management Action. ITSD management stated:

   "IT Services agrees with this finding.

   "IT Services is recruiting a Chief Information Security Officer and one of their duties will be to update the County's Information Technology Disaster Recovery Policy and Standards document, which will reflect any needed updates to policy and procedure, as well as the suggested revision log.

   "Estimated Completion Date: March 31, 2020"

8. **Vendor Contract Terms.** Contracts with outside vendors to provide disaster recovery-related services and equipment existed but did not always contain all recommended clauses to protect the County's interests. We noted various areas of recommended improvement regarding the content of vendor agreements and the timing of contract services as specified below.

   A. **Vendor Agreement Content.** Each of the four vendor agreements was missing one or more of the following clauses recommended to protect the County's interests:

      - Penalties to the vendor if services are not provided, or not provided timely.
      - Designated alternate site location(s) that correlates to location(s) identified within the DRP.
      - A clause to ensure non-disclosure and protection of County data.
      - A "right to audit" clause allowing the County to inspect the vendor's books and records.

      Agreements missing any of the information noted above may put the County at risk of inappropriate data disclosure and/or being unable to recover critical systems within required timeframes.

      Recommendation. ITSD management should coordinate with the General Services Agency Procurement Division to determine whether the above items are necessary in current and/or future contracts.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services will coordinate with the General Services Agency Procurement Division to establish a disaster recovery vendor agreement template.

"Vendors typically do not agree to be subject to penalties for services not provided due to natural disasters.

"Estimated Completion Date: December 31, 2019"

B. **Timing of Vendor Services.** Of the four vendor agreements reviewed, two did not state when services would be provided and the other two specified service timelines that might not align with the County's operational needs. The mobile data center contract stated delivery will take 48 to 72 hours, and the contract for replacement equipment stated delivery will take 1 to 5 business days. Should any of the County's vital systems (e.g., public safety, health care, etc.) require restoration of ITSD managed systems in less than one business day, the current contracts would not provide the County with the necessary resources.

Recommendation. ITSD management should verify if vendor service timelines coincide with business operational requirements to restore system functionality. If a vendor's service timelines do not meet the department's operational requirements, ITSD management should either seek amendments to the vendor contract or adjust restoration expectations accordingly.

Management Action. ITSD management stated:

"IT Services agrees with this finding.

"IT Services will review vendor agreements to confirm service timelines meet the department's requirements. However, vendors typically do not agree to shorter timelines, which may vary depending on the specific disaster.

"In addition, IT Services is currently defining a redundant virtual environment and redundant backup solutions to be housed in a separate location from the primary data center. This redundant solution will provide remediation without the possibility of utilizing either of the contracts mentioned above.

"Estimated Completion Date: December 31, 2019"

AUDITOR'S EVALUATION OF MANAGEMENT ACTION

We believe that management actions taken or planned were responsive to the audit findings. ITSD management planned to complete corrective actions by June 30, 2020.