County of San Diego Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

CLOUD COMPUTING AUDIT

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Mady Cheng, CPA, CIA, CISA, MSBA
Auditor II: Wasim Akand, MPA

Report No. A14-034

March • 2015

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

March 24, 2015

TO: Mikel Haas, Chief Information Officer
County Technology Office

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: CLOUD COMPUTING AUDIT

Enclosed is our report on Cloud Computing 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 Wasim Akand at (858) 694-2248.

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

JUAN R. PEREZ
Chief of Audits

AUD:WA:aps

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Damien Quinn, Group Finance Director, Finance and General Government Group
Andrew McDonald, Group IT Manager, Finance and General Government Group
Dorothy Gardner, IT Contract Manager, Finance and General Government Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of Cloud Computing. The objective of the audit was to assess the cloud computing strategy and governance functions to ensure effective management processes, risk management practices, and monitoring of cloud provider performance.

Background

The cloud computing model is a method of procuring and deploying information technology (IT) resources and applications using only a network connection. According to the National Institute of Standards and Technology (NIST),[1] cloud computing is “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

The NIST definition lists five essential characteristics of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The NIST also lists three "service models" (software, platform, and infrastructure), and four "deployment models" (private, community, public, and hybrid) that together categorize ways to deliver cloud services.

The County of San Diego (County) utilizes a hybrid cloud approach. Primary uses of cloud computing within the County are for software as a service (SaaS) and/or infrastructure as a service (IaaS), in which applications, servers and storage are hosted in a cloud service provider (CSP) data center and where County data is processed and/or stored.

In February 2013, the Cloud Review Committee (CRC), a subgroup of the IT Governance Group (ITGG), which is part of the County’s IT governance hierarchy, established a governance framework over the acquisition of CSP services. The CRC is comprised of Group Information Technology Managers (GITMs) and County Technology Office (CTO) staff. The purpose of this Board is to review new cloud services requested by County departments, assess risk against established and agreed-to criteria and processes, and, if appropriate, make recommendations to the IT Management Committee (ITMC) for acceptance or rejection of those CSP requests considered high-risk. It is not the role of the CRC to manage the acquisition of cloud services, review or approve contract documents, or to monitor the service providers. These responsibilities are owned by Purchasing & Contracting (DPC), County Counsel, and the County departments acquiring the services.

[1] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, dated Sept 2011.

The CRC created a "2-Track Process" to eliminate inconsistencies and streamline the CSP approval process, and to ensure that contract documentation is sufficient to pass certain technical reviews. The 2-Track process establishes separate approval procedures for new and renewed CSP contracts, depending on the risk level. For the CRC, risk under their purview is directly related to the nature of the data and the services to be provided. The CRC does not evaluate risk against the presence or absence of certain CSP contract provisions. Low risk CSPs must be approved only by the CRC, while high risk CSPs must be approved by both the CRC and the ITMC. All CSPs, regardless of procurement method, must be vetted through the 2-Track Process.

Audit Scope & Limitations

The scope of the audit included the County's IT governance structures, risk management practices, and monitoring processes over CSPs for fiscal year 2013-14. The CRC, DPC, County Counsel, and selected County departments were included in this assessment. Required CSP forms and approval processes, as documented in the CSP Request Procedure (CoSD-C001), were evaluated as of the control effective date of February 2013.

This 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.

OAAS also based their assessment on *recommended* IT controls from the IT Governance Institute's *Control Objectives for Information and related Technology* (COBIT) framework[2] and the NIST SP 800-53 *Guide for Assessing the Security Controls in Federal Information Systems and Organizations.*[3]

Methodology

OAAS performed the audit using the following methods:

- Reviewed IT control *frameworks* such as COBIT and NIST and best practices relating to cloud computing deployment.

- Reviewed the CTO Cloud Computing Strategy Recommendation Document, and CSP policies and procedures related to cloud computing governance and security.

- Interviewed the CRC and CTO management on processes and procedures relevant to CSP contract inventory maintenance and risk management practices.

- Reviewed IT Project Management Office (ITPMO) Cloud Service Provider List maintained by the CRC and interviewed County

[2] COBIT is ISACA's framework for the management and governance of business-driven IT-based projects and operations.

[3] NIST SP 800-53 – The NIST IT security controls standards contain a controls framework required to address cloud security.

department personnel to verify completeness and adequacy of the inventory.

- Judgmentally selected a sample of six CSP contracts from the ITPMO Cloud Service Provider List for detailed review. Sample selection was based on risk level (high, medium, low), cost of service, and cloud service type.

- Reviewed relevant documentation such as CSP contracts, terms of service, and service level agreements (SLA)[4] to determine if cloud service contracts defined CSP security and performance requirements.

- Interviewed County department personnel responsible for each sampled CSP contract to verify whether the department:

  - Monitored CSP performance and security as outlined in contract and SLA.

  - Obtained and reviewed third-party assessment reports, such as the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 16[5] report, and/or security assurances, such as ISO 27001 Certification.[6]

AUDIT RESULTS

Summary

The County has made significant progress towards adopting cloud computing technologies; however, opportunities exist to further strengthen the IT governance framework over cloud computing. Improvement opportunities were identified in the areas of CSP contract management, monitoring of CSP performance, and CSP risk management.

Finding I: CSP Contract Terms Should Be Strengthened

The CSP contracts sampled did not always address certain recommended key contract provisions including:

- **Contractual Audit Rights**

  - **Right-to-Audit Clause**: Of the six contracts sampled, two did not include a "right-to-audit" clause, including one high risk contract. The right-to-audit clause ensures that the County has access to audit the CSP and verify the existence and effectiveness of controls specified in the CSP contract and associated SLA.

[4] A service level agreement is a contract between a service provider and customer that specifies, in measurable terms, what services the provider will furnish.

[5] SSAE 16 is a regulation created by the AICPA defines how service companies report on compliance controls.

[6] ISO27001 Certification provides service provider security assurance.

COBIT recommends "assess the status of external service providers' internal controls. Confirm that controls comply with legal and regulatory requirements and contractual obligations".

Without a right-to-audit clause included in the CSP contract, the County may not be able to obtain assurance that the vendor is in compliance with the contract or SLA if the need arises.

- **Independent Third-Party Review and Security Certification:** The CSP contracts for all six sampled CSPs did not include a requirement that CSPs periodically provide an independent third-party assessment, such as an SSAE 16 report or an ISO 27001 security certification.

  COBIT recommends that independent audit and assurance of the completeness and effectiveness of internal controls at the outsourced providers be obtained to confirm that agreed-on requirements are being adequately addressed.

  Failure to ensure appropriate internal controls at the CSP could result in higher costs, fines, service interruption, or unauthorized access to County data resulting in data loss or compromise.

- **Service Level Agreements**
  Two CSP contracts sampled did not include SLAs. Three other contracts that had SLAs defined did not specify penalties should CSP performance fall below required SLA thresholds. SLAs define, in measurable terms, the acceptable service levels to be provided by the CSP, service quality, and timeliness of services provided under the contract. SLAs provide the basis against which the County is able to manage service provider performance.

  COBIT recommends that SLAs should be defined and agreed to by the service provider and the customer for all critical IT services based on customer requirements.

  The County takes on increased risk if the contract does not hold the CSP accountable for substandard or non-performance based on the SLA requirements. The consequences to the County if an SLA is not met could seriously impact services provided by the County.

Other than the SLAs defined in the IT Outsourcing Agreement, there was no other contract template or defined criteria for County departments to reference when reviewing CSP contracts to ensure that appropriate SLAs and other recommended contract provisions are included. When provided to Counsel; however, Counsel does review the agreements against certain County requirements (e.g., liability) to ensure adequate protections are in place.

Without guidance on recommended provisions for inclusion in CSP contracts, the lack thereof in the contract terms and conditions may increase the risk that cloud services will not meet County requirements potentially resulting in inadequately performing and unsecure or unavailable services.

Recommendation: To improve management and oversight of cloud computing services, OAAS recommends that the CRC, together with DPC and County Counsel identify standard recommended contract provisions and key criteria and provide those to County departments when they are evaluating providers and reviewing subsequent CSP contracts and SLAs. This will help ensure that the departments procuring the services are aware of these recommended provisions in their CSP agreements and understand and accept the risks should they decide not to include them.

At a minimum, the following provisions should be addressed by the departments:

1. A right-to-audit clause that allows the County to conduct specific security and internal control audits at a CSP location that cannot be restricted or curtailed by the CSP.

2. An annual independent third-party assessment and/or security certification provided to the County upon request. County departments should ensure that:

    a. The CSP contract commits to an annual security certification such as ISO 27001 and/or an annual independent third-party audit such as an SSAE 16.

    b. The third-party assessment provided by the CSP includes a description of the IT controls in place at the CSP and an assessment of the design; operating effectiveness of the controls; and CSP follow-up action plans to address issues reported.

3. Specific, measurable, and enforceable SLA performance and availability requirements and thresholds are defined in the contract and include defined penalties should CSP performance fall below required SLA thresholds.

The CRC, in its role, should ensure that departments are apprised of the need for the above, consider them in their evaluation of the CSP, and, if the department determines that any of the provisions are not needed, that decision by the department is documented and maintained in the records of the CRC.

Finding II: **CRC Documentation of Risk Management Practices Can Be Strengthened**

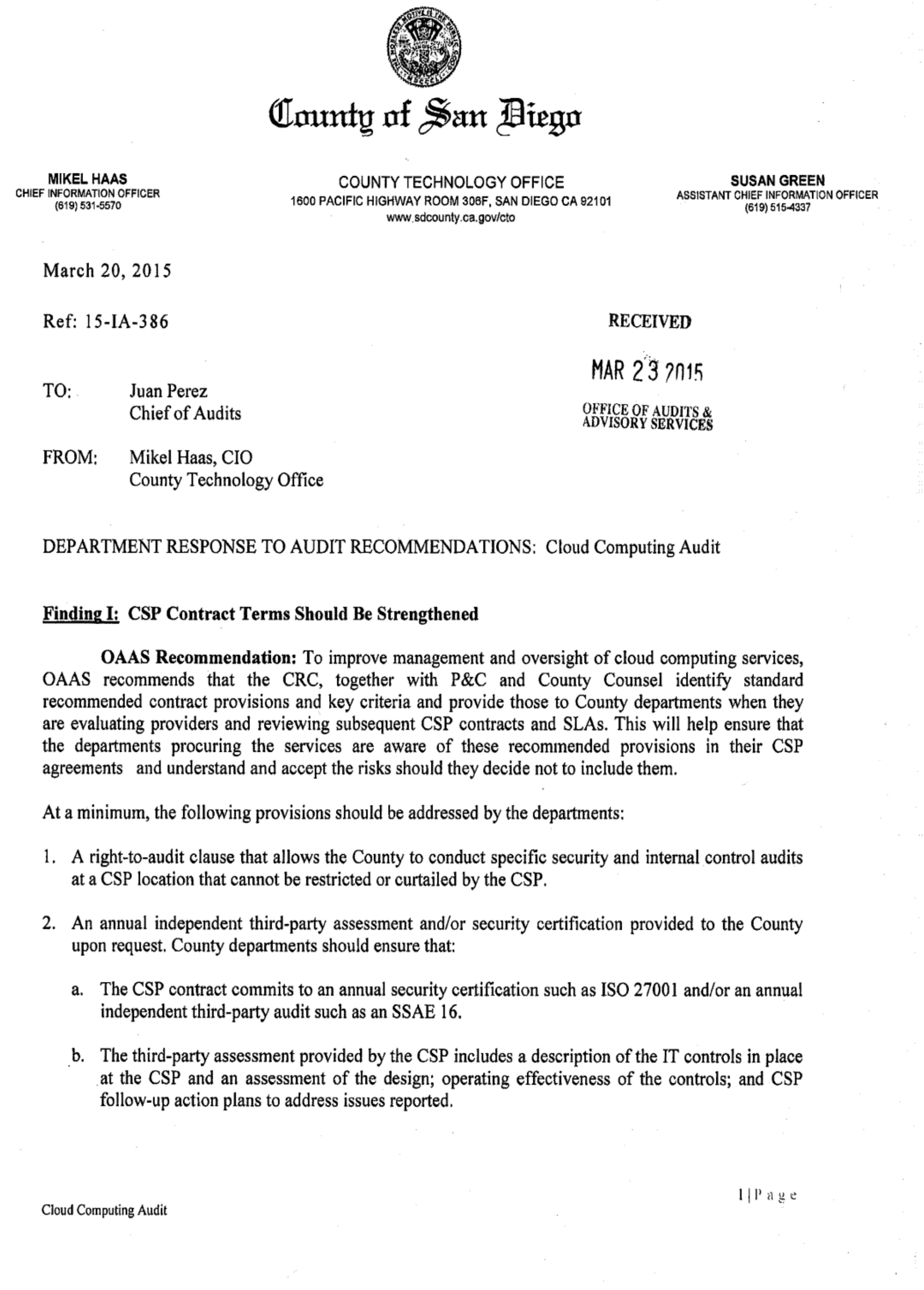
Although the CRC performs an informal risk assessment for each procured cloud service, there is no risk assessment document produced to evidence the risks identified, the results of the assessment, or agreed upon mitigating controls that address and manage the risks identified. Effective risk management requires that CSP contracts address how contractor and subcontractor performance will be managed and security, privacy, and data management requirements will be met.

COBIT recommends that risk relating to a suppliers' ability to continually provide secure, efficient, and effective service delivery should be identified and managed. Relevant data that could play a significant role in the management of IT risk should be recorded and an inventory of known risk and the control activities maintained to manage risk.

Without a documented risk assessment, it may be difficult to determine if all risks have been identified, appropriate actions taken to mitigate the risks or evidence of County management approval of action plans to address risks. County data may be at risk of being hosted by a CSP with inadequate controls over data security, availability, integrity, confidentiality and privacy.

Recommendation: The CRC review and approval process for CSP contracts should include documenting identified risks and agreed upon mitigating controls established by the CSP vendor and subcontractors, and approved by department management.

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

March 20, 2015

Ref: 15-IA-386

TO: Juan Perez
Chief of Audits

FROM: Mikel Haas, CIO
County Technology Office

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: Cloud Computing Audit

Finding I: CSP Contract Terms Should Be Strengthened

OAAS Recommendation: To improve management and oversight of cloud computing services, OAAS recommends that the CRC, together with P&C and County Counsel identify standard recommended contract provisions and key criteria and provide those to County departments when they are evaluating providers and reviewing subsequent CSP contracts and SLAs. This will help ensure that the departments procuring the services are aware of these recommended provisions in their CSP agreements and understand and accept the risks should they decide not to include them.

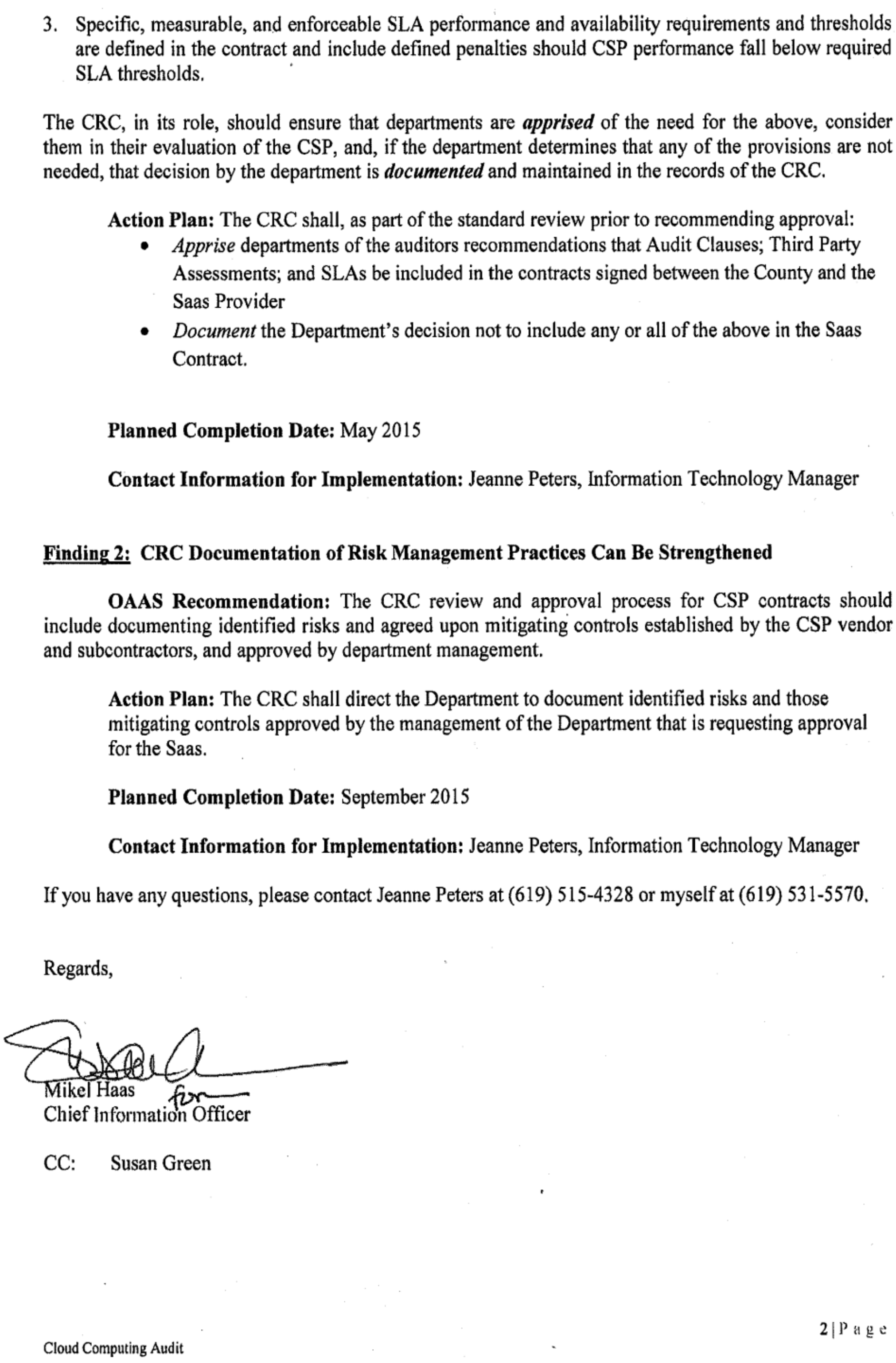
At a minimum, the following provisions should be addressed by the departments:

1. A right-to-audit clause that allows the County to conduct specific security and internal control audits at a CSP location that cannot be restricted or curtailed by the CSP.

2. An annual independent third-party assessment and/or security certification provided to the County upon request. County departments should ensure that:

   a. The CSP contract commits to an annual security certification such as ISO 27001 and/or an annual independent third-party audit such as an SSAE 16.

   b. The third-party assessment provided by the CSP includes a description of the IT controls in place at the CSP and an assessment of the design; operating effectiveness of the controls; and CSP follow-up action plans to address issues reported.



3. Specific, measurable, and enforceable SLA performance and availability requirements and thresholds are defined in the contract and include defined penalties should CSP performance fall below required SLA thresholds.

The CRC, in its role, should ensure that departments are ***apprised*** of the need for the above, consider them in their evaluation of the CSP, and, if the department determines that any of the provisions are not needed, that decision by the department is ***documented*** and maintained in the records of the CRC.

Action Plan: The CRC shall, as part of the standard review prior to recommending approval:

- *Apprise* departments of the auditors recommendations that Audit Clauses; Third Party Assessments; and SLAs be included in the contracts signed between the County and the Saas Provider
- *Document* the Department's decision not to include any or all of the above in the Saas Contract.

Planned Completion Date: May 2015

Contact Information for Implementation: Jeanne Peters, Information Technology Manager

<u>Finding 2:</u> CRC Documentation of Risk Management Practices Can Be Strengthened

OAAS Recommendation: The CRC review and approval process for CSP contracts should include documenting identified risks and agreed upon mitigating controls established by the CSP vendor and subcontractors, and approved by department management.

Action Plan: The CRC shall direct the Department to document identified risks and those mitigating controls approved by the management of the Department that is requesting approval for the Saas.

Planned Completion Date: September 2015

Contact Information for Implementation: Jeanne Peters, Information Technology Manager

If you have any questions, please contact Jeanne Peters at (619) 515-4328 or myself at (619) 531-5570.

Regards,

Mikel Haas for
Chief Information Officer

CC: Susan Green