Information Technology Cyber Security
Internal Controls Assessment

June 2021

ORANGE COUNTY SANITATION DISTRICT

Submitted By:

Eide Bailly LLP

David Rowan, CPA, CSSFP, ISO 27001 Lead Auditor
Senior Manager, Risk Advisory Services

Audrey Donovan, CIA, CGAP, CRMA
Senior Manager, Risk Advisory Services

Roger Alfaro, CPA, CITP
Partner

TABLE OF CONTENTS

Executive Summary 3

Objective & Scope.....3

Methodology 3

Results of Internal Controls Assessment 4

Finding #1:

Users access is not reviewed on a regular basis for network access or for general applications.....5

Finding #2:

No formal Vendor Management Policy and Program is in place.....6

Finding #3:

Policies and procedures are not updated on an annual basis.....7

Executive Summary

Eide Bailly LLP ("we", "our" or "us") was engaged by Orange County Sanitation District ("OCSD") to conduct a controls assessment of OCSD's Information Technology Cyber Security Controls and adherence with documented policies and procedures. Eide Bailly evaluated the adequacy of existing processes, procedures, and internal controls within the Information Technology Department.

The assessment included review of OCSD's written policies and procedures (P&Ps), interviews of key personnel from the Information Technology Department, detailed testing of Cyber Security processes, and review of supporting documentation. The assessment identified both strengths, weaknesses and risks related to processes, procedures, and internal controls. We provided three (3) findings and their associated recommendations related to improvement opportunities or additional considerations that may be necessary to properly and adequately address risks and achieve business objectives.

Objective & Scope

The objective of the project was to provide OCSD with an internal assessment of OCSD's Information Technology Cyber Security Controls and adherence with documented policies and procedures. The Scope of the assessment focused on the following overarching cyber elements generally associated within the IT control environment as well as cyber specific application elements within the "significant systems" scoped by management: JD Edwards, IBM Maximo, PM Web, and Blue Beam:

- Security Management
- Access Control
- Configuration Management & Software Development
- Segregation of Duties
- Contingency Planning and Computer Operations
- Incident Management and Response
- Physical Security
- Application Interface Management

Our service was provided in accordance with the American Institute of Certified Public Accountants' Statement on Standards for Consulting Services and do not constitute an examination or review of the subject matter. Accordingly, we will not express an opinion or conclusion on the subject matter. Lastly, OCSD management determined that vulnerability and penetration testing would not be in scope for this project, as they are performed regularly by management.

Methodology

Procedures performed during this assessment included the following 4 (four) areas:

1. **Systems Review** – Gained an understanding of the General IT Control environment as well as the internal systems in scope including JD Edwards, IBM Maximo, PM Web, and Blue Beam and the controls designed to mitigate the risks associated with each application.
2. **Assessment of Internal Controls and Procedures** – Gained an understanding and assessed the adequacy of existing internal procedures and associated risks regarding compliance with internal procedures and specific cyber related threats within the environment.
3. **Compliance Testing** – Obtained and reviewed policies, procedures, configurations, and performed operational effectiveness testing for 50 General Cyber Security Controls, and 65 application specific controls for JD Edwards, IBM Maximo, PM Web, and Blue Beam covering the following the following cyber domains:
    - Security Management

- Access Control
- Configuration Management & Software Development
- Segregation of Duties
- Contingency Planning and Computer Operations
- Incident Management and Response
- Physical Security
- Application Interface Management

Results of Internal Controls Assessment

OCSD's Information Technology Cyber Security Control environment is a mature technology environment utilizing appropriate infrastructure for the size and scope of the industry, configurations reviewed are designed to mitigate the threats OCSD faces in a complex and ever-changing cyber landscape. There are a number of well-designed controls, but as is typical in control environments, formalization of these controls in policy and procedure could be updated on a consistent basis that we recommend be formally reviewed and approved at least annually. In summary, the issues and concerns noted during the assessment were related, but not limited to the following:

- Users access is not reviewed on a regular basis for network access or for general applications.
- No formal Vendor Management Policy and Program is in place.
- Policies and procedures are not updated on an annual basis.

In conclusion, we greatly appreciate and thank the input of all OCSD stakeholders in this project who contributed to enhancing our understanding of OCSD's Technology Cyber Security Control environment as well as identifying opportunities for process improvements. We hope and believe that, at a minimum, addressing and resolving the findings and recommendations provided in this independent assessment would directly and positively contribute and add value to the overall efficiency and effectiveness of the Information Technology Department.

Findings & Recommendations

Based on the procedures performed, it appears OCSD has many of the necessary internal controls in place to mitigate potential risks within its Cyber Security Control environment. We have provided three (3) findings and their associated recommendations in this report related to improvement opportunities or additional considerations that may be necessary to properly and adequately address risks and achieve business objectives. These recommendations were designed to strengthen current controls, improve oversight of operations, increase overall efficiency and effectiveness of Cyber Security Control environment, and reduce compliance risks for OCSD.

Finding #1: Users access is not reviewed on a regular basis for network access or for general applications
Risk Rating: Medium

1.1 There is not a formal user access review performed by OCSD to review the network users or any application specific users throughout the environment.

Recommendation #1:

1.1 OCSD should formalize the user review process to review all users for network and key applications at least on an annual basis. Review should include the following:

- Comparison of Network User listing to Current Employee listing to verify users are active employees. Further examination of these users should verify–with their appropriate supervisors–the groups users are associated with to reduce risk of users having access to potential confidential user access.
- Comparison of Application User listings to Current Employee listing to verify users are active employees. Further examination of these users should verify–with their appropriate supervisors–the roles within the applications to ensure access is distributed on the basis of least privilege.

OCSD's Response:

OCSD to formalize the user review process for user network and application access. Work with the different application groups to create/modify annual review process for user access. Expected time for resolution is 3-6 months.

Finding #2: No formal Vendor Management Policy and Program is in place
Risk Rating: Low

2.1 OCSD currently has a process in place to onboard new vendors into their system through their website and perform limited security assessments upon onboarding. There is currently not a process to obtain independent assessments on these vendors and currently there is no regular review of a vendor's security posture based on risk on a regular basis.

Recommendation #2:

2.1 OCSD should formalize a vendor management program to not only evaluate vendors risk posture upon onboarding of the vendor utilizing an independent third party, they should also classify their current vendors based on risk and determine a strategy to review these vendors on a periodic basis, with high risk vendors being assessed at least annually.

OCSD's Response:

OCSD to evaluate a third-party vendor risk management solution and create a strategy for periodic review process. Expected time for resolution is 6-12 months.

Finding #3: Policies and procedures are not updated on an annual basis
Risk Rating: Low

3.1 The following policy and procedure documentation have not been reviewed in the last year and one such policy was last reviewed 10 years prior according to the internal date stamp on the policy:

1. Change and release management Policy
2. Patch management policy does not exist within Information Security Policy
3. Electronic Communications Policy
4. IT Job descriptions
5. Mission Essential Functions (Business Impact Analysis)
6. Backup and Restoration Policy
7. Disaster Recovery and Incident Response Policy

Recommendation #3:

3.1 Technology changes at a rapid pace and associated policies should reflect these changes as the controls are updated to address the risks identified by OCSD and the actions needed to mitigate the risks throughout the environment. We recommend that all policies within the Information Technology department be reviewed at least annually.

OCSD's Response:

OCSD to review and update IT policies annually and create new policies where applicable. Expected time for resolution is 4 months.

Caring for our external and internal clients with a passion to go the extra mile.

Respecting our peers and their individual contributions.

Conducting ourselves with the highest level of integrity at all times.

Trusting and supporting one another.

Being accountable for the overall success of the Firm,
not just individual or office success.

Stretching ourselves to be innovative and creative, while managing the related risks.

Recognizing the importance of maintaining a balance between work and home life.

Promoting positive working relationships.

And, most of all, enjoying our jobs ... and having fun!

EideBailly®

What inspires you, inspires us.

eidebailly.com