Orange County Sanitation District
IT Governance Audit
September 2025

VASQUEZ
+ COMPANY LLP

Orange County Sanitation District
IT Governance Audit
September 2025

VASQUEZ
+ COMPANY LLP

655 N. Central Avenue
Suite 1550
Glendale, CA 91203

www.vasquez.cpa

213-873-1700
OFFICE

\ LOS ANGELES
\ SAN DIEGO
\ IRVINE
\ SACRAMENTO
\ FRESNO
\ PHOENIX
\ LAS VEGAS
\ MANILA, PH

September 15, 2025

To the Management and Board of Directors
Orange County Sanitation District
Fountain Valley, CA 92708

Dear Ladies and Gentlemen:

We are pleased to present the results of the Information Technology (IT) Governance Audit conducted for the Orange County Sanitation District (OC San) covering the period from June 1, 2024, to May 31, 2025. This audit was performed in accordance with the internal audit plan and was designed to evaluate the effectiveness of OC San's IT governance framework, cybersecurity practices, and related internal controls.

The audit procedures and methodology were developed with consideration of the results of the enterprise-wide risk assessment process and the approved audit plan.

This report summarizes our observations and offers valuable insight into the current state of OC San's IT governance environment, highlighting both strengths and opportunities for improvement.

This report is intended solely for the information and use of Management and the Board of Directors of OC San. It is not intended to be, and should not be, used by any other parties without prior authorization.

We appreciate the opportunity to support OC San in its continued efforts to strengthen its IT governance and cybersecurity resilience.

Very truly yours,

VASQUEZ & COMPANY, LLP

Roger A. Martinez
Partner

EXECUTIVE SUMMARY

Vasquez & Company, LLP (Vasquez) was engaged by the Orange County Sanitation District (OC San) to assess OC San's Information Technology Governance and its related processes and controls. The evaluation focused on the effectiveness of the design and implementation of current processes, procedures, and internal controls within the IT Department.

The assessment covered IT processes within the defined scope and included a review of OC San's documented policies and procedures, interviews with key IT personnel, testing of the design and implementation of IT and cybersecurity practices, and examination of relevant supporting documentation. The review identified both strengths and areas for improvement, along with associated risks. As a result, three (3) key observations were presented, each accompanied by recommendations aimed at enhancing risk management and supporting the achievement of OC San's operational goals.

OBJECTIVE & SCOPE

The purpose of this engagement was to conduct an internal evaluation of OC San's Information Technology and Cybersecurity governance, controls, and their compliance with established policies and procedures. The scope of the assessment focused on key technology and cybersecurity components based on NIST (National Institute of Standards and Technology) Cybersecurity Framework 2.0. Test of design and effectiveness focused on the "critical applications" identified by management: JD Edwards, Active Directory, and SentinelOne.

The following key domains were covered by this assessment:

- IT Governance and Risk Management
- Program Change Management
- User Access Management
- IT Operations
- Cyber and Physical Security

METHODOLOGY

1. Reviewed OC San's control environment, including key business processes and critical IT systems as it relates to IT Governance.

2. Assessed risk factors associated with key IT processes and critical systems:
    a. Alignment with Business Goals
    b. Risk Management
    c. Change Management
    d. Information Security
    e. Technology Obsolescence
    f. Transparency and Accountability
    g. IT Vendor Management

3. Conducted an IT governance assessment, evaluating compliance with IT and cybersecurity policies and procedures across the following sub-domains:

    a. IT Risk Assessment Activities
    b. IT Strategic Planning
    c. Information Security Awareness Training and Programs
    d. IT Vendor and Third-party Risk Management
    e. Change Management Processes
    f. User Provisioning, Modification, Termination, and Periodic Access Reviews
    g. Anti-virus, Firewall, and Patch Management
    h. Backup and Recovery Procedures
    i. Data Protection Measures
    j. Incident Management Processes
    k. Physical Security Controls

4. Performed controls testing and evaluation to determine the effectiveness of existing IT controls.

AREAS OF STRENGTH

The assessment, which focused on critical systems and key IT and cybersecurity domains, revealed that key controls tested are operating effectively as designed and are aligned with OC San's IT operations and risk management strategies. Below are the notable areas of strength:

1. OC San has implemented key cybersecurity controls such as antivirus, firewall, and patch management systems. These measures contribute to a robust defense against cyber threats and demonstrate proactive risk mitigation.

2. OC San has shown clear recognition of their exposure to emerging IT and cybersecurity risks. The IT Department remains attentive to identified threats and focuses its efforts on initiatives that contribute to the integrity of OC San's IT environment. OC San's openness to formalizing its policies, updating documentation and enhancing segregation of duties shows a proactive stance in strengthening internal controls.

3. While some documents are recommended to be formalized, the presence of internal IT guidelines demonstrates OC San's awareness of standardized processes and controls, to ensure that these align with organizational goals, security standards and regulatory requirements.

RESULT OF INTERNAL CONTROL ASSESSMENT

While no significant deficiencies or material weaknesses were identified during the audit, some areas were noted where IT Governance practices can be enhanced to further improve IT oversight and align with leading practices. Each observation is accompanied by practical recommendations designed to strengthen existing controls, clarify roles and responsibilities and enhance policy implementation. The following details the observations, the suggested recommendations and Management's responses:

Observation #1:

During the walkthrough performed for program change management, and as later confirmed with IT Management, it was determined that there was no segregation of duties between the functions of code development and promotion of code to Production within the JD Edwards application. It was also noted that no independent review process was in place to ensure that no unauthorized, inadequate, or excessive changes were promoted to Production.

In addition, testing of sample changes implemented during the audit period revealed instances where segregation of duties was not consistently observed. Specifically, there were instances where the same individual acted as both developer and tester or as both developer and implementer, which weakens the control over the change management process:

1. Normal Change
   a. CHG0032024 – The Developer and Tester were the same person.

2. Standard Change
   a. CHG0031864 & CHG0031650 – The Developer and Implementer were the same person.

Risk Rating: Medium

Risk Description:

When a single individual performs a combination of the three key change management functions - development, testing and implementation - there is an increased risk that unauthorized, inadequate, or excessive changes may be implemented in the Production environment, whether due to error or potential fraud.

Recommendation:

1. Consider assigning the functions of code development, testing, and promotion to Production to different personnel.

2. If segregation of duties is not feasible due to the nature of the organization or for other reasons, consider assigning other personnel to perform activities such as a pre-deployment or post-deployment check to mitigate the risks of unauthorized changes being deployed to Production.

Given the crucial nature of development, testing, and implementation to Production activities, segregating these three responsibilities is essential to minimizing the risk of unauthorized, inadequate, or excessive changes due to fraud or errors. When segregation is not practical, using audit trails to track all change activities and requiring an independent review can serve as effective compensating controls.

OC San's Response:

When feasible, OC San Supervision will assign different personnel to the development, testing and implementation of changes to production systems. Optimally, the testing will be performed by the end user to verify that the change has been implemented successfully. If the prior two options are not feasible, IT will perform a post-deployment check.

Observation #2:

During the operating effectiveness test of change management controls, no evidence was provided to support the following key testing details related to four (4) sampled change requests:

a. Developer
b. Date Submitted for Testing
c. Actual Testing Date
d. Tested By
e. Testing Result

The four sample tickets identified were:
a. Normal Change – CHG0032024
b. Normal Change – CHG0031965
c. Standard Change – CHG0031872
d. Standard Change – CHG0031631

Risk Rating: Medium

Risk Description:

The absence of evidence to support the testing procedures for each change request increases the risks of unverified deployment of changes to Production. This can potentially lead to higher project costs, delays, and security-related challenges.

Recommendation:

Retain evidence of testing procedures performed for each change request. At a minimum, the following details must be clearly stated in the supporting documentation:

a. Developer
b. Date Submitted for Testing
c. Actual Testing Date
d. Tested By
e. Testing Result

If it is not feasible to retain the above documentation within the change request tickets, consider creating a separate repository to store and maintain all relevant supporting documentation.

Retaining complete documentation of testing procedures is essential to prevent OC San from incurring heavy delays and experiencing security issues arising from Production changes that do not function as intended, which can ultimately lead to additional costs. Maintaining a complete change log is also key to identifying opportunities to improve efficiency within the change management process.

OC San's Response:

Change management in IT is documented in the IT Service Management (ITSM) solution. Modifications to the ITSM change management module will be implemented and will require the developer's name, date submitted for testing, actual testing date, the tester's name, and the test results be entered prior to closing the change request. Staff will have the ability to attach screenshots to support the change request.

OC San management believes the risk is partially mitigated by reviewing all changes on a weekly basis during the Change Advisory Board (CAB) meeting. The CAB mitigates risk by bringing multiple perspectives into decision-making, enforcing structured reviews, ensuring contingency planning, and aligning changes with business needs. Every change request reviewed by the CAB goes through a formal risk/impact analysis. This ensures consideration of:

- Business continuity
- Cybersecurity implications
- System dependencies
- Regulatory compliance
- Timing considerations
- Rollback plan

Observation #3:

We noted the following observations regarding OC San's IT policies and guidelines:

1. A formal board-approved IT policy and IT guidelines exist, covering the following areas:

    a. User Access Management
    b. Program Change Management
    c. Disaster Recovery
    d. Incident Response
    e. Information Security

    However, not all the documents relating to the above are current or show evidence of their most recent review.

2. Although the Wireless/Electronic Communications/Acceptable Use of IT policy mentions the use of passwords within OC San, it does not define specific password settings in any written policy or guidelines document.

Risk Rating: Low

Risk Description:

Without clear, formally documented, and approved policies and procedures, confusion may arise regarding the appropriate processes, controls, and procedures to be followed. The lack of uniform guidelines increases the risk of inconsistent application of control procedures across teams, particularly within the OC San's critical IT processes.

Recommendations:

1. Conduct regular reviews of IT policies/guidelines (typically on an annual basis) and formally document the results and any updates to ensure they remain reflective of OC San's IT practices.

2. Consider revisiting the scope of each policy/guideline to determine whether the following key IT processes are adequately covered:

    a. User Access Management (including password management)
    b. Program Change Management
    c. IT Risk Management
    d. Backup and Restoration
    e. Disaster Recovery Plan/Business Continuity Plan
    f. Incident Handling/Problem Management
    g. Information Security Policy (if separate from the above)

    Based on the above, existing policies/guidelines may be merged or new ones developed and clearly classified either as board-approved policies or IT team guidelines.

Developing and maintaining comprehensive policies and guidelines for key IT areas is essential in ensuring consistent and efficient implementation of IT practices across OC San. Establishing a periodic review and approval process for IT policies and guidelines helps determine if these are reflective of current processes and remain relevant to address the evolving IT risk environment. In addition, by establishing a formal review and approval process for policies and procedures, control owners will have a higher sense of responsibility over compliance with established controls.

OC San's Response:

An ITSM ticket will be created with an annual reoccurrence and assigned to the IT Manager to review the IT policies and guidelines. All policies and guidelines will have notations identifying the last date changed and reviewed. Where applicable, IT processes will be added and updated to the OC San Wireless Electronic Communications policy. New IT guidelines will be created to cover key IT processes.

*****

This communication is intended solely for the information and use of OC San's Management and Board of Directors and is not intended to be, and should not be, used by anyone other than these specified parties.

Vasquez & Company LLP

Glendale, California
September 15, 2025

www.vasquez.cpa

655 N Central Avenue, Suite 1550 • Glendale, California 91203-1437 • +1.213.873.1700