OC SAN
ORANGE COUNTY SANITATION DISTRICT

IT Governance Audit Results

INTERNAL AUDIT SERVICES

September 24, 2025

VASQUEZ
+ COMPANY LLP

/ Table of Contents

IT Governance Risk Factors and Scope	2
Audit Program Framework	3
Audit Results Summary	4
Observation 1	5
Observation 2	6
Observation 3	7
Questions	8
Contact Information	9

VASQUEZ + COMPANY LLP

/ IT GOVERNANCE RISK FACTORS AND SCOPE

Risk Factors	Audit Scope
• **Alignment with Business Goals** • **Risk Management** • **Change Management** • **Information Security** • **Technology Obsolescence** • **Transparency and Accountability** • **IT Vendor Management**	The following procedures were performed to assess the actions taken by Orange County Sanitation District (OC San) to address the identified IT Governance Risk Factors: a. Inspected Strategic Plans, IT Roadmaps, and Governance structures to confirm whether IT initiatives are prioritized and executed in alignment with business objectives. b. Assessed the design and effectiveness of established IT Policies and Procedures by testing control areas such as Access Management, Program Change Management, and IT Operations. c. Reviewed the processes for selecting, managing, and monitoring third-party vendors to ensure that due diligence is performed and that vendors are regularly evaluated. d. Reviewed OC San's IT processes for continuously monitoring risks such as cybersecurity threats, compliance issues, and performance failures. **In-scope Systems:** JD Edwards, Active Directory, SentinelOne **Covered Period:** June 01, 2024 - May 31, 2025

/ AUDIT PROGRAM FRAMEWORK

Vasquez & Company (Vasquez) developed an IT Governance Audit work program to assess OC San's IT Governance and Risk Management Controls.

Vasquez leveraged **NIST Cybersecurity Framework 2.0 (CSF 2.0)**, which is structured around six core Functions: **Govern, Identify, Protect, Detect, Respond, and Recover**.

The NIST CSF 2.0 served as the basis of our assessment, encompassing five (5) areas within the scope of the audit:

1. IT Governance and Risk Management
2. Program Change Management
3. User Access Management
4. IT Operations
5. Cyber and Physical Security

VASQUEZ
+ COMPANY LLP

/ AUDIT RESULTS SUMMARY

Based on the results of the procedures performed, the controls tested are operating effectively as designed, **except** for the following observations:

IT Process	Category	Description
Program Change Management	**Medium**	Observe Segregation of Duties Between Change Developers, Testers, and Implementers
	Medium	Retain Evidence of Testing Procedures Performed Per Change Request
IT Governance and Risk Management	**Low**	Develop, Review, and Update IT Policies and Guidelines

Based on our assessment, the identified deficiencies in OC San's internal controls did not constitute significant deficiencies or material weaknesses.

Notes:

- **High** – An observation of potential significance to the overall control environment; Affects multiple systems/components; Impact is pervasive; Requires the immediate attention of management to define a priority action plan for its resolution (within 3 months).
- **Medium** – An observation of moderate significance to the overall control environment; Affects one system/component; Impact is not pervasive; Requires the near-term attention of management and an agreed program for its near-term resolution (6 months to 1 year).
- **Low** – An efficiency or administrative observation of lesser significance; Does not warrant immediate attention; However, requires an agreed program for ultimate resolution, depending on the organization's assessment.

VASQUEZ + COMPANY LLP

1 / IT AUDIT OBSERVATIONS & RECOMMENDATIONS

Description	Observe Segregation of Duties Between Change Developers, Testers, and Implementers		
IT Process	Program Change Management	Category	Medium
Observations		**Risks**	
It was determined that code development, testing, and promotion of code to Production in the JD Edwards application were not segregated.		Lack of Segregation of Duties in the Change Management process increases the risk of having unauthorized, inadequate, or excessive changes implemented in Production due to fraud or errors.	
Recommendations			
1. If feasible, assign the functions of code development, testing, and promotion to Production to different personnel. 2. Implement pre-deployment or post-deployment checks to mitigate risks of unauthorized changes being deployed to Production.			

VASQUEZ + COMPANY LLP

2 / IT AUDIT OBSERVATIONS & RECOMMENDATIONS

Description	Retain Evidence of Testing Procedures Performed Per Change Request		
IT Process	Program Change Management	Category	Medium
Observations		**Risks**	
Insufficient evidence was provided to support the following key testing details for four (4) sample change requests: a. Developer b. Date Submitted for Testing c. Actual Testing Date d. Tested By e. Testing Result		Missing key change information increases the risks of unverified deployment of changes to Production, potentially leading to higher costs, project delays, and security issues.	
Recommendations			
Retain evidence of development and testing procedures performed for each change request. If the information cannot be retained in the ticketing system, consider creating a separate repository.			

3 / IT AUDIT OBSERVATIONS & RECOMMENDATIONS

Description	Develop, Review, and Update IT Policies and Guidelines		
IT Process	IT Governance and Risk Management	Category	Low
Observations		**Risks**	
1. Not all the IT Policies and Guidelines are current or show evidence of their most recent review 2. Specific password settings are not defined in any written policy or guideline		Lack of uniform guidelines increases the risk of inconsistent application of control procedures across teams, particularly within OC San's critical IT processes.	
Recommendations			
Review policies and guidelines periodically (typically annually) and document the results or any suggested changes to ensure they remain reflective of OC San's IT practices. Part of the periodic review should include assessing the need to create new documentation, IT policies and guidelines, to address evolving IT risks.			

/ Questions

VASQUEZ
+ COMPANY LLP

/ Contact Information

Vasquez + Company LLP has over 55 years of experience in performing audit, accounting, and consulting services for all types of private companies, nonprofit organizations, and governmental entities.

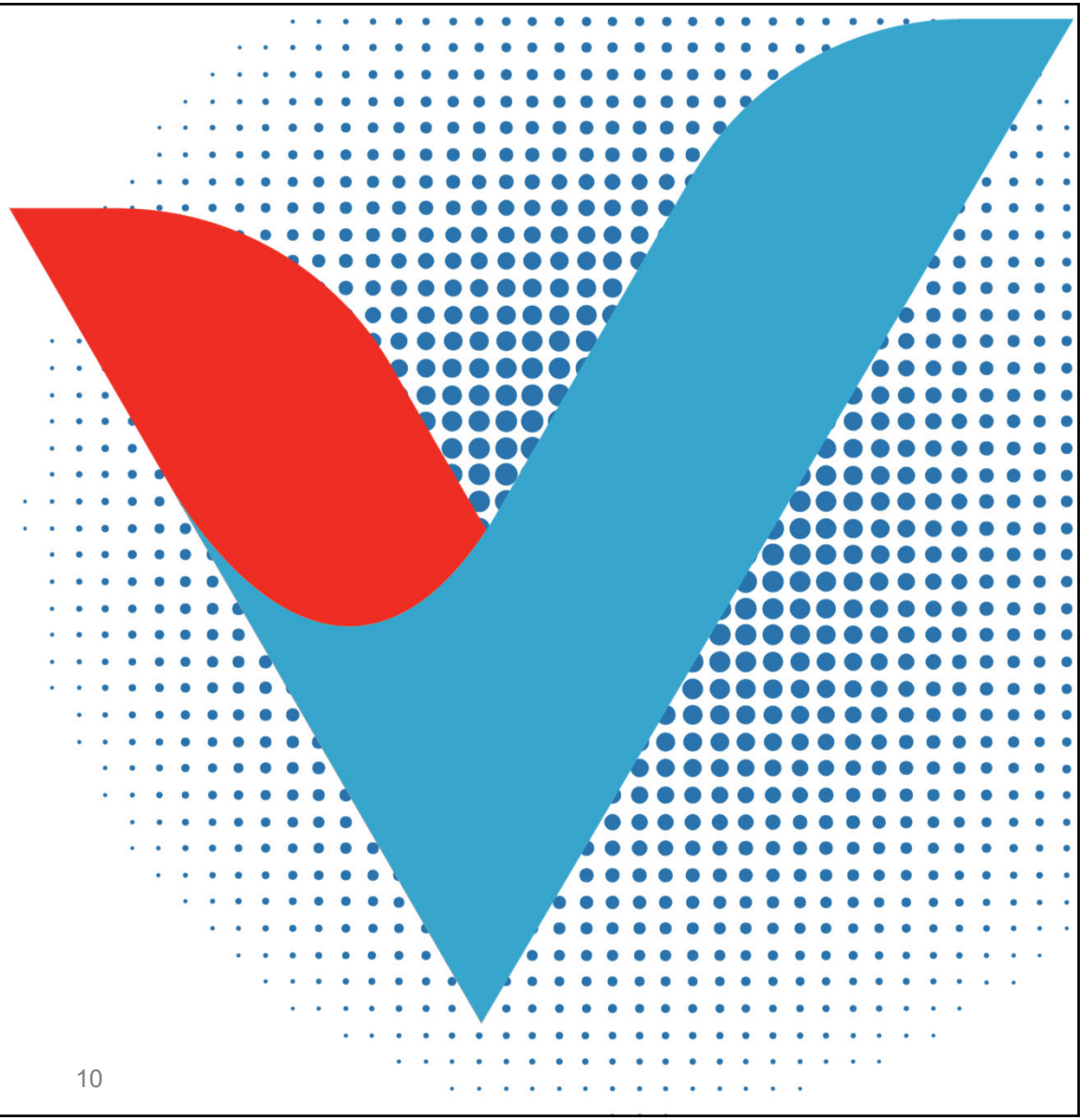
We are clients of the **Aprio Professional Services+ Practice**. As a client, we have access to the Professional Services+ Collaborative, a globally connected community that provides access to an ecosystem of capabilities, collaboration and camaraderie to help professional services firms grow and thrive in a rapidly changing business environment. As a participant in the PS+ Collaborative, we have the opportunity to interact and share best practices with other professional services firms across the U.S. and Canada.

Roger Martinez, CPA
O: +1.213.873.1703
ram@vasquezcpa.com

Arcely Peran, CPA
O: +1.213.873.1731
aperan@vasquezcpa.com

Jason Tagasa, CISA
O: +1.213.873.1773
jtagasa@vasquezcpa.com

www.vasquez.cpa

VASQUEZ
+ COMPANY LLP

Thank you for your time and attention.