Orange County Sanitation District
Enterprise Risk Assessment
April 23, 2025

Orange County Sanitation District
Enterprise Risk Assessment
April 23, 2025

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

April 23, 2025

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

Dear Ladies and Gentlemen:

We are pleased to present this Enterprise Risk Assessment (ERA) and Proposed Audit Plan for the Fiscal Years 2025 – 2029 for Orange County Sanitation District (OC San or the Organization). The basis of the Proposed Audit Plan was developed by considering the results from the recent risk assessment process performed, the previously approved risk assessment and audit plan prepared in July 2022, results of audits completed since the previous audit plan was approved and the approved budget for internal audits.

This document serves as the primary work plan to carry out the responsibilities of Internal Audit. This plan is not intended to be static or unchangeable. Changes in conditions, emerging risks, or special requests may require changes to the Proposed Audit Plan. The final Audit Plan will be determined by the Audit Ad Hoc Committee of the Board of Directors, and it may require changes to the approved internal audit budget.

This report is intended solely for the information and use of the Audit Ad Hoc Committee, Board of Directors, and management and is not intended to be, and should not be, used by anyone other than these specified parties. It will be our pleasure to respond to any questions you have about this report. We appreciate the opportunity to continue to be of service to the Orange County Sanitation District.

Very truly yours,

VASQUEZ & COMPANY, LLP

Roger Martinez

Roger Martinez
Partner

Table of Contents

ENTERPRISE RISK ASSESSMENT

Vasquez & Company LLP (Vasquez) follows the guidance of the International Professional Practices Framework (IPPF) issued by the Institute of Internal Auditors. The IPPF standards emphasize that internal audit plans should be risk-based and align with the organization's goals. These plans must be found on a documented risk assessment, updated periodically, and should incorporate input from management and the Audit Ad Hoc Committee.

What is an Enterprise Risk Assessment?

An enterprise risk assessment is a comprehensive process that helps organizations identify, assess, and manage risks across all departments and business units, ensuring a holistic approach to risk management and compliance.

It involves using professional judgment to evaluate risk factors and their effects on the entity. Risk factors refer to the relevant information that significantly affects how the identified risk is managed, prioritized, monitored, and reported. This may include the following:

- Results of prior period internal audit reports
- Size and significance of the affected department operations
- Effects on operations
- Regulatory requirements
- Financial exposure
- Volume of transactions
- Vulnerability to fraud
- Effectiveness of the internal control system

An enterprise risk assessment is designed to enable management, governance, and other key stakeholders to identify and agree on the key risks facing OC San through a rigorous process of discovery and assessment.

Risk Assessment Methodology

Vasquez created a tailored risk assessment approach for OC San's departments, people, and processes. The process begins with planning and scoping to steer the risk assessment, followed by developing risk types, measures, and risk scores.

To identify and understand current emerging risk areas, Vasquez conducted interviews and discussions with members of the governance and management of OC San. Vasquez also reviewed the information provided by OC San, including organizational charts, regulatory reports, strategic plans, minutes of board meetings, financial statements, and results of past internal audits. The information gathered from the interviews, along with documents reviewed, was utilized to develop the Enterprise Risk Assessment Results and Proposed Audit Plan.

RISKS IDENTIFIED

Risk arises when there are internal and/or external forces that could negatively affect the fundamentals that drive OC San's objectives, strategies, and values in the services provided to its customers. Future changes in environmental factors and actions by personnel that cannot be anticipated may significantly and adversely impact risk exposure.

This risk assessment identified sixteen (16) risks applicable to OC San:

1. **Talent Acquisition:** The risk associated with an organization's difficulty in acquiring suitable workers with the requisite skill set to meet the organization's workforce needs.

2. **Talent Retention:** The risk associated with an organization's difficulty in retaining top-performing employees to meet or sustain the organization's workforce needs.

3. **Succession Planning:** The risk associated with an organization's difficulty in maintaining its normal operations in the event of the loss of key or critical personnel. The need for a comprehensive, enterprise-wide succession planning process impacts OC San's business continuity, may lead to potential knowledge loss, employee turnover, and cultural impairment, and could result in a struggle to execute the organization's strategic objectives.

4. **Physical Security of Assets:** The risk associated with the vulnerability of the organization's assets against internal and/or external threats that may result in the loss or destruction of property and/or disruption of services to customers.

5. **Supply Chain:** The risk associated with the potential disruption of an organization's operational flow of goods and services, which may result in delays of projects, delayed maintenance, and losses being incurred.

6. **Vendor Management:** The risk in vendor management refers to the potential for adverse outcomes resulting from the organization's reliance on third-party vendors. It encompasses any threat that could arise from the vendor's actions, inactions, or external factors affecting the vendor's ability to deliver services or products as expected.

7. **Construction Projects (Project and Budget Management):** The risk associated with potential disruption on the execution of construction projects, such as delays, construction incidents, backlogs, and cost overruns, including significant differences or changes between the actual cost of materials or projects and estimated costs.

8. **Business Continuity:** The risk associated with the organization's vulnerability or struggle to continue operating at normal capacity and provide essential services during or after a major and/or prolonged disruptive event.

9. **Generative AI:** The risk associated with the organization's vulnerability related to data security and inappropriate or over-reliance on information generated using Artificial Intelligence.

10. **Cybersecurity Vulnerabilities:** The risk associated with the organization's vulnerability to cyber-attacks such as hacking, the infestation of malware, viruses & ransomware, phishing, social engineering, and others. Lack of robust ongoing cybersecurity efforts across the organization to keep up with changes and advances in external attacker capabilities and threats could lead to theft of employee or customer information, including personally identifiable information (PII) and/or intellectual property. Security breaches may result in business disruption, reputational harm, lawsuits, and financial loss.

11. **Technology Obsolescence Risk:** The risk associated with the organization's obsolescence of IT infrastructure, such as equipment, platforms, programs, and software. IT applications and infrastructure, including various disparate systems that do not interface or integrate, may limit visibility and transparency of information across the organization, thereby inhibiting the organization’s ability to make informed business decisions and achieve its strategic objectives.

12. **IT Governance:** The risk associated with the misalignment between IT strategy and business objectives, which can lead to security vulnerabilities and negatively impact organizational performance.

13. **Regulatory Complexity:** The risk associated with the organization's vulnerability or struggle to readily comply with the dynamic changes and legislation advances of regulatory requirements, which may result in fines and/or penalties and, under worst-case scenarios, disruption of operations. An example of these regulatory requirements includes those related to the management of hazardous waste, such as biosolids, micro-plastics, and Polyfluoroalkyl Substances (PFAS), which, if improperly discarded or managed, might result in harm to consumers, the community, or the environment.

14. **Workplace Safety:** The risk associated with workplace hazards that may lead to injuries, illness, or damage, including but not limited to exposure to harmful substances, electrical, and fire hazards.

15. **Reputation:** The risk associated with a negative view of the organization by the public due to regulatory noncompliance and shortcomings in delivering its promise to protect health and the environment by providing effective wastewater collection, treatment, and recycling.

16. **Rights and Obligations:** The risk associated with an organization's struggle to consistently enforce its rights and to acknowledge its obligations. This may include inconsistently monitoring and handling assets and obligations for items such as easements.

Risk Score

Assignment of risk scores and ratings involved professional judgment. To determine the significance of the risks identified, Vasquez combined the ***impact***, should it occur, and the ***likelihood*** or the probability of the risk's occurrence. Risk scores and ratings are assigned to both impact and likelihood; the average of which is determined to be the Final Risk Score and ***Final Risk Rating***.

- **Impact** refers to the magnitude to which an identified risk may affect the Organization. The impact is determined through a combination of considerations that a certain risk may significantly affect the Organization's operations, financial health, reputation, safety, and significant areas of the Organization.

- **Likelihood** refers to the probability that a certain event will occur. Likelihood is often described using qualitative terms such as likely, possible, unlikely, rare, or as a percentage of probability.

RISK AREA SCORING MATRIX

Risk Area Scoring Matrix Risks Identified	Impact Score	Likelihood Score	Final Risk Score
Human Capital Risks			
Talent Acquisition	9	3	6
Talent Retention	6	6	6
Succession Planning	9	9	9
Business / Operations			
Resources and Supplier			
Physical Security of Assets	9	3	6
Supply Chain	9	9	9
Vendor Management	6	9	7.5
Operational			
Construction Projects (Project & Budget Management)	9	6	7.5
Business Continuity	9	5	7
Information Technology			
Generative AI	9	9	9
Cybersecurity Vulnerabilities	9	9	9
Technology Obsolescence Risk	9	9	9
IT Governance	9	6	7.5
Regulatory/ Safety/ Reputation/ Legal Risks			
Regulatory Complexity	6	6	6
Workplace Safety	6	6	6
Reputation	3	1	2
Rights and Obligations	6	6	6

Risk Rating	Risk Score	Risk Definition
High	> 7.51	Poses a significant financial reporting or operational risk, will most likely require ongoing sustained resources, includes accounting issues or balances that include significant estimates or judgments.
Medium	4.51 to 7.50	Poses a moderate financial reporting or operational risk, will involve less resources, involves fewer complex controls and accounting issues.
Low	1 to 4.50	Minimal financial reporting or operational risk, requires low level of resources, routine control and accounting issues.

RISK HEAT MAP

Risk Identified	Departments														
	Governance	General Manager	Financial Management	Contracts, Purchasing, & Materials Management	Information Technology	Facilities Management	Communications Department	Human Resources Administration	Risk Management	Environmental Services Administration	Resource Protection	Environmental Compliance	Engineering Department	O&M Department	Plant 1&2 Operations
Human Capital Risks															
Talent Acquisition															
Talent Retention															
Succession Planning															
Business / Operations															
Resources and Supplier															
Physical Security of Assets															
Supply Chain															
Vendor Management															
Operational															
Construction Projects (Project & Budget Management)															
Business Continuity															
Information Technology															
Generative AI															
Cybersecurity Vulnerabilities															
Technology Obsolescence Risk															
IT Governance															
Regulatory/ Safety/ Reputation/ Legal Risks															
Regulatory Complexity															
Workplace Safety															
Reputation															
Rights and Obligations															

ENTERPRISE RISK ASSESSMENT RESULTS

From the Risk Heat Map, identified risks are listed below in accordance with the determined risk rating, along with the details related to noted key trigger points and respondent departments.

Risk Identified	Key Trigger Points	Risk Rating	Departments
Human Capital			
Talent Acquisition	• Inconsistency in the competitiveness of the salary and benefits package for certain positions as compared to the industry • Tenured personnel leaving/retiring • Some understaffing noted in upper level of management, especially in the O&M department	Medium	• Human Resources Administration
Talent Retention	• Inconsistency in the competitiveness of the salary and benefits package for certain positions as compared to the industry • Tenured personnel leaving/ retiring	Medium	• Financial Management • Resource Protection • Environmental Compliance • Plant 1 & 2 Operations
Succession Planning	• Inconsistency in competitiveness of salary and benefits package for certain positions as compared to industry • Tenured personnel leaving/ retiring • Personnel that are the only source of knowledge regarding key processes • Some understaffing noted in upper level of management, especially in the O&M department	High	• Governance • Financial Management • Facilities Management • Human Resources Administration • Risk Management • Resource Protection • Environmental Compliance • Engineering Department • O&M Department • Plant 1 & 2 Operations

Risk Identified	Key Trigger Points	Risk Rating	Departments
Business/ Operations			
Resources and Supplier			
Physical Security of Assets	• Drones as a risk to physical access • Potential acts of terrorism • Structural integrity/ resilience of the plants and facilities against seismic activities • Buildings and facilities requiring maintenance • Adequacy of current physical security (security guards and cameras) • Theft, vandalism, and destruction of property	Medium	• Governance • Information Technology • Human Resources Administration • Risk Management
Supply Chain	• Significant lead time on receipt of supply • Contractors' delay is experienced in procurement • Contractors not performing in accordance with the agreed level or quality of work • Expense payment and income collection processes need upgrades.	High	• Governance • General Manager • Financial Management • Engineering Department
Vendor Management	• Contractors are not performing as agreed upon • Robust enforcement of contracts agreed upon • Making sure contracts are in OC San's best interest • Over- or under-reliance on consultants, suggesting the need for clear guidelines and accountability	Medium	• General Manager • Financial Management • O&M Department • Plan 1 & 2 Operations

Risk Identified	Key Trigger Points	Risk Rating	Departments
Operational			
Construction Projects (Project and Budget Management)	• Delays in project designs and executions • Incomplete / Delayed projects costing more money and time • Cost estimates that are significantly different from actuals • Contractors not performing as agreed upon.	Medium	• Governance • Facilities Management • Environmental Services Administration • Environmental Compliance
Business Continuity	• Business continuity amidst crisis or natural catastrophes • Structural integrity/ resilience of the plants and facilities against seismic activities • Buildings and facilities requiring maintenance • Power outages • Equipment and facilities with limited alternative replacement options, higher cost of replacement, and/ or higher cost of repairs; This may cause the Organization to be unable to operate at maximum level.	Medium	• Governance • Contracts, Purchasing, & Materials Management • Engineering Department • Plant 1 & 2 Operations

Risk Identified	Key Trigger Points	Risk Rating	Departments
Information Technology			
Generative AI	• Planned integration of AI in operations/ processes • Developing memorialized guidelines for the use of AI	High	• Governance • General Manager • Financial Management • Contracts, Purchasing, & Materials Management • Information Technology • Communications Department • Human Resources Administration • Resource Protection • Engineering Department
Cybersecurity Vulnerabilities	• Use of third-party Software as a Service (SaaS) • Vulnerability related to attacks on a third-party SaaS vendor • Cloud-based storage	High	• Governance • Information Technology • Facilities Management • Communications Department • Human Resources Administration • Risk Management • Engineering Department
Technology Obsolescence Risk	• Risk of software obsolescence related to legacy systems • Shift to virtual timecards	High	• General Manager • Information Technology
IT Governance	• Use of third-party SaaS • Vulnerability related to attacks on a third-party SaaS vendor	Medium	• General Manager • Financial Management • Information Technology • Communications Department

Risk Identified	Key Trigger Points	Risk Rating	Departments
Regulatory/ Safety/ Reputation/ Legal Risks			
Regulatory Complexity	• The complexity of new regulatory requirements related to waste management, such as PFAS and biosolids	Medium	• Governance • Financial Management • Environmental Services Administration
Workplace Safety	• Workplace safety vs. outcomes • Incidents are expensive and often avoidable • Sufficiency of safety policies and procedures	Medium	• Governance
Reputation	• Potential for the negative viewpoint of the public/ affected community on OC San's delivery on promises and obligations	Low	• Governance • Communications Department
Asset Management - Rights and Obligations	• Unaccounted properties from prior years, including obligations such as easement rights • Possibility of unknown properties as noted by the prior year's external auditor	Medium	• Governance • Communications Department • Predecessor Auditor

PROPOSED AUDIT PLAN

The Proposed Audit Plan outlines the suggested Internal Audit engagements for the next five-year period. It is important to note that the Proposed Audit Plan is a working document that should be flexible in addressing current priorities in a changing environment. The Audit Ad Hoc Committee will review and approve any significant additions, deletions, or other changes in the Proposed Audit Plan prior to modification. Annual review and approval of purchase orders is required.

The methodology used to create the list of eight proposed audits below was as follows:

- We did not propose an audit for low-risk areas
- We proposed audits for all high and medium risk areas, and we evaluated whether they should have recurring audits in the 5-year period (all IT related areas have recurring audits on the schedule, other proposed audits for multiple years relate to either other high risk areas or breaking apart the procedures due to scope size)
- We combined certain audit risk areas into one proposed audit category as follows:
    - Human Capital Management includes all 3 risk areas identified (succession planning, talent acquisition, and talent retention); we suggest focusing on succession planning, as that is the high-risk area of the three, for the first proposed audit in FY 25-26 and the talent acquisition and talent retention areas for the second proposed audit in FY 28-29
    - We combined physical security of assets, business continuity, and rights and obligations under the Asset Management proposed audits for FY 27-28 and FY 29-30 (divided into two separate proposed audits to stay within budget)
    - We combined technology obsolescence risk, vendor management, and IT governance in the proposed audit IT Governance - Vendor, Asset, and Change Management
    - The proposed Workplace Safety audit also includes the risks related to regulatory complexity
    - The proposed audit Construction Project and Budget management also includes risks related to vendor management

Proposed Audits FY 25-26 through FY 29-30

The table below summarizes the proposed FY 25-26 through FY 29-30 internal audits, activities, estimated timing, and risk rating discussed and validated through the risk assessment process. Please note that two audits have been approved for FY 25-26, and any additional audits may require an adjustment to the approved budget.

No.	Proposed Audits	Final Risk Rating	Fiscal Years				
			25-26	26-27	27-28	28-29	29-30
1	Human Capital Management	High/ Medium	X			X	
2	IT Cybersecurity Vulnerabilities	High		X		X	
3	IT Generative AI	High		X		X	
4	Supply Chain	High		X			X
5	IT Governance - Vendor, Asset, and Change Management	High/ Medium	X		X		X
6	Construction Projects and Budget Management	Medium			X		
7	Workplace Safety	Medium	X				
8	Asset Management	Medium			X		X

Details of Proposed Audits FY 25-26 through FY 29-30

The proposed audits will cover the following areas:

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
1	Human Capital Management	• **Leadership Vacuum:** A significant risk is the potential for a leadership vacuum if key leaders leave unexpectedly without suitable successors in place. • **Skill Gaps:** When experienced personnel depart, there is a risk of losing valuable institutional knowledge and expertise. • **Challenges in Onboarding:** New employees may find it more difficult to get up to speed without access to the accumulated knowledge of their predecessors. • **Regulatory Compliance:** New leaders may lack the necessary understanding of regulatory requirements, leading to potential non-compliance issues. • **Selecting the Wrong Candidate:** Absence of a well-defined succession planning process increases the likelihood of selecting an unsuitable candidate for a position. • **Compensation and Benefits:** Inconsistency in competitiveness of the salary and benefits package for certain positions as compared to the industry	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified Human Capital Management Risk Factors: **Proposed Audit No. 1 – Succession Planning:** a. Assess the Organization's succession planning framework to ensure it includes key elements such as identification of critical roles, talent assessment, development plans, and contingency strategies. b. Review implementation of knowledge transfer strategies, such as adequacy of training, mentorship program, and documentation of best practices, to help preserve critical information. **Proposed Audit No. 2 – Talent Acquisition and Retention:** a. Assess the Organization's current leadership structure to identify vacant positions, roles with unclear responsibilities, and areas where leadership is deficient.

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
			b. Evaluate the quality and readiness of the Organization’s internal talent pool including reviewing the skills, competencies, and potential of identified successors. c. Review of the Organization’s current pay structures, benefits offerings, and related policies to ensure they are effective, competitive, and compliant with legal regulations.
2	IT Cybersecurity Vulnerabilities	• **Data Breaches:** Vulnerabilities can be exploited to gain unauthorized access to sensitive data. • **Malware and Ransomware:** These threats can disrupt operations and cause significant financial losses. • **Insider Threats:** Employees or contractors with legitimate access can misuse their privileges. • **Denial of Service (DoS) Attacks:** These attacks can overwhelm systems, making them unavailable to users. • **Software Vulnerabilities:** Unpatched software can be exploited by attackers.	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified IT Cybersecurity Vulnerability Risk Factors: a. Examine the Organization's security policies and procedures to ensure they are comprehensive and up-to-date and address key areas such as access control, incident response, and data protection. b. Evaluate the Organization's mission-critical information system to identify potential security weaknesses. c. Assess the procedures taken by the Organization to test and scan mission-critical information systems to uncover vulnerabilities that could be exploited by cyber threats, verify compliance with relevant laws and industry standards, and provide actionable insights to improve the organization's security posture.

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
			d. Assess the Organization's tools and techniques used for monitoring user activities, such as event logs and automated solutions.
3	IT Generative AI	• **Data Privacy and Security:** Generative AI systems often require large amounts of data, which can include sensitive information. • **Bias and Fairness:** AI models can inadvertently learn and perpetuate biases present in the training data. • **Model Integrity:** Generative AI models can produce inaccurate or misleading outputs, known as "hallucinations." • **Ethical and Legal Compliance:** The use of generative AI can raise ethical and legal concerns, such as intellectual property issues and compliance with regulations. • **Operational Risks:** Integrating generative AI into business processes can introduce operational risks, such as system failures or performance issues.	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified IT Generative AI Risk Factors: a. Assess the Organization's policies and guidelines for the use of generative AI. b. Evaluation of the performance and accuracy of AI models, c. Verification that data privacy and protection measures are in place and comply with regulations. d. Examination of how generative AI is integrated into workflows and systems. e. Assessment of the quality and reliability of AI-generated outputs. f. Determination of potential biases in AI outputs and ensuring measures are in place to mitigate them.
4	Supply Chain	• **Supplier Reliability:** Dependence on a single supplier can be risky if they face disruptions. This may include risks related to delays, significant lead time for receipt of supply, vulnerability to price changes, and unsatisfactory quality of supply.	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified Supply Chain Risk Factors: a. Review the Organization's practices and policies to ensure supplier diversification, including criteria for selecting and evaluating

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
		• **Logistics Disruptions:** Transportation delays, port congestion, and accidents can disrupt the supply chain. • **Regulatory Compliance:** Changes in regulations can impact supply chain operations.	suppliers (sufficiently diversified across different regions, industries, and risk profiles), and managing supplier relationships. b. Supplier's compliance with contractual obligations and performance standards. Review of regulatory changes and comparison to supplier information to determine whether there are risks of noncompliance or disruption. c. Review KPIs related to logistics, such as delivery times, order accuracy, and cost efficiency, and conduct tests to ensure logistics plans are effective and can adapt to changes in demand or supply chain disruptions.
5	IT Governance – Vendor, Asset, and Change Management	• **Alignment with Business Goals**: IT initiatives may not align with the overall business strategy, leading to wasted resources and missed opportunities. • **Risk Management**: Inconsistently identifying and managing IT risks can lead to significant disruptions. • **Compliance:** Non-compliance with regulatory requirements can result in legal penalties and reputational damage. • **Resource Constraints and Obsolescence:** Limited resources can hinder the effective implementation of IT governance. The risk of obsolescence could lead to disruption in	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified IT Governance – Vendor, Asset, and Change Management Risk Factors: a. Evaluate the Organization's IT environment maturity by evaluating the clarity and effectiveness of roles and responsibilities among the IT Organization and assessing established IT Policies and Procedures. Assess the effectiveness of the IT Policies and Procedures by testing control areas such as Access Management, Program Change Management, and IT Operations. b. Evaluate if the Organization has identified outdated or soon-to-be-obsolete technology within the Organization and assess the risks

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
		operations or struggle to meet strategic objectives. • **Transparency and Accountability:** A lack of transparency and accountability in IT decision-making can lead to inefficiencies and mismanagement. • **Vendor Risks:** Vendors and partners can introduce vulnerabilities into your systems.	and impacts of using such technology, including security vulnerabilities, inefficiencies, and compliance issues. Evaluate how the Organization manages the changes and implementation of the new systems. c. Assess the processes for selecting and managing third-party vendors and ensure that due diligence is performed and that vendors are regularly evaluated. d. Assess the Organization's processes for continuously monitoring third-party vendors to manage risks such as cybersecurity threats, compliance issues, and performance failures.
6	Construction Projects and Budget Management	• **Budget/Cost Overruns:** Projects often exceed their budgets due to unforeseen expenses not included in cost estimation. • **Unscheduled Delays:** Delays can occur due to various factors such as weather conditions, supply chain disruptions, or labor. • **Cost Deviations:** Significant deviations from cost estimates can disrupt ongoing operations, especially if funds need to be diverted from other critical areas to cover the shortfall, or the change in estimates was not factored into long-term rate adjustments. • **Quality Control Issues**: Ensuring that construction meets the required standards is crucial.	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified Construction Projects and Budget Management Risk Factors: a. Review of cost estimation and approval process. b. Review the approval and ongoing monitoring of the budget and spending associated with projects. c. Review the internal and external quality control processes in place to ensure that construction standards are met.

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
		• **Regulatory Compliance:** Adhering to local, state, and federal regulations can be challenging and time-consuming, but non-compliance can result in significant fines and project delays.	d. Review key performance indicators (KPIs) and other metrics to assess the project's progress, efficiency, and effectiveness.
7	Workplace Safety	• **Exposure to Hazards:** These include potential slips, trips, falls, machinery accidents, electrical hazards, poor workstation design, stress, harassment, workplace violence, and exposure to hazardous substances that can cause health issues. • **Defects:** Errors during operation can lead to unsafe water treatment and/or waste management, which may expose the OC San, the community, and the environment to hazards. • **Compliance with Standards:** Failure to adhere to safety standards and regulations can increase the risk of product-related injuries and legal liabilities. • **Compliance Costs:** New regulations often require significant investments in technology and processes to meet compliance standards. • **Environmental and Public Health Concerns:** Any inconsistencies in disposal methods can lead to environmental contamination, affecting soil, water, and air quality.	The following proposed audits and procedures will assess the actions taken by the Organization to address the identified Workplace Safety Risk Factors: a. Conduct surveys or interviews with employees to gather information about their perceptions of workplace safety and any concerns they may have about violence or threats and potential hazards. b. Evaluate existing safety procedures and protocols to assess their effectiveness and whether these are followed correctly, and if they are adequate to mitigate identified hazards. c. Examine records of regulatory filings, permits, and incident reports to ensure compliance with environmental and public health standards. d. Analyze employee and community complaints and feedback to identify recurring safety, health, and environmental issues and areas needing improvement. e. Evaluate metrics and reports on safety and compliance for newly implemented projects.

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
8	Asset Management	• **Unauthorized Access:** Preventing unauthorized individuals from entering secure areas is crucial. • **Risk of Theft and Vandalism:** Physical theft and vandalism can result in significant financial losses and property damage. • **Insider Threats:** Employees or contractors with legitimate access can pose risks if they misuse their access. • **Natural Disasters:** Events like earthquakes, floods, and fires can disrupt operations and damage facilities. • **Inconsistent Property Recordkeeping:** Inconsistent recordkeeping of rights and obligations related to property can result in reputational harm and potential liability, financial loss, and fines.	The following proposed audit procedures will assess the actions taken by the Organization to address identified Management, Rights, Obligations, and Monitoring Risks Factors: **Proposed Audit No. 1 – Asset Security and Access Rights:** a. Test implementation of access control systems, including key cards, biometric scanners, and security personnel to mitigate security risk. b. Review the effectiveness of installed surveillance cameras, alarm systems, and physical barriers such as fences and locks in deterring unauthorized activities. c. Evaluate policies for conducting background checks, and monitoring access logs, including evaluation of whether access controls are functioning correctly, and only authorized users can access sensitive data. d. Verify if the roles and responsibilities of the business continuity team and other stakeholders are clearly defined and understood, and assess the effectiveness of internal and external communication plans, ensuring contact lists are current and communication channels are established.

No.	Proposed Audits	Risk Factors	Proposed Audit Scope
			Proposed Audit No. 2 – Asset Monitoring, Rights, and Obligations: a. Evaluate the asset monitoring process and validate that the controls are working effectively, ensuring all assets are recorded. b. Examine deeds, easement agreements, and other legal documents to verify the entity's rights to use the property and any obligations associated with it. c. Compare internal records with external documents, such as land registry records, to ensure consistency and accuracy in the reporting of easements and property ownership.

CONCLUSION

The Enterprise Risk Assessment for the Orange County Sanitation District (OC San) has identified critical risks and proposed a comprehensive audit plan to address these challenges over the next five years. This assessment underscores the importance of proactive risk management and the need for continuous monitoring and adaptation to emerging threats and opportunities.

The identified risks highlight areas where OC San must focus its efforts to ensure operational resilience and compliance. The proposed audit plan provides a structured approach to mitigate these risks, enhance internal controls, and support OC San in achieving its strategic objectives.

It is ultimately up to the Audit Ad Hoc Committee to decide which risks need to be prioritized and how soon the audits should be performed. The dynamic nature of risks necessitates that this audit plan remains flexible, allowing for adjustments in response to changing conditions and new insights. Additionally, there may be a need to modify the approved internal audit budget to accommodate the Audit Ad Hoc Committee's requests.

We are confident that the enterprise risk assessment results and proposed audit plan presented in this report will serve as a valuable resource for OC San's management and governance bodies. We look forward to supporting OC San in its ongoing efforts to enhance risk management practices and achieve excellence in service delivery.

www.vasquez.cpa

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