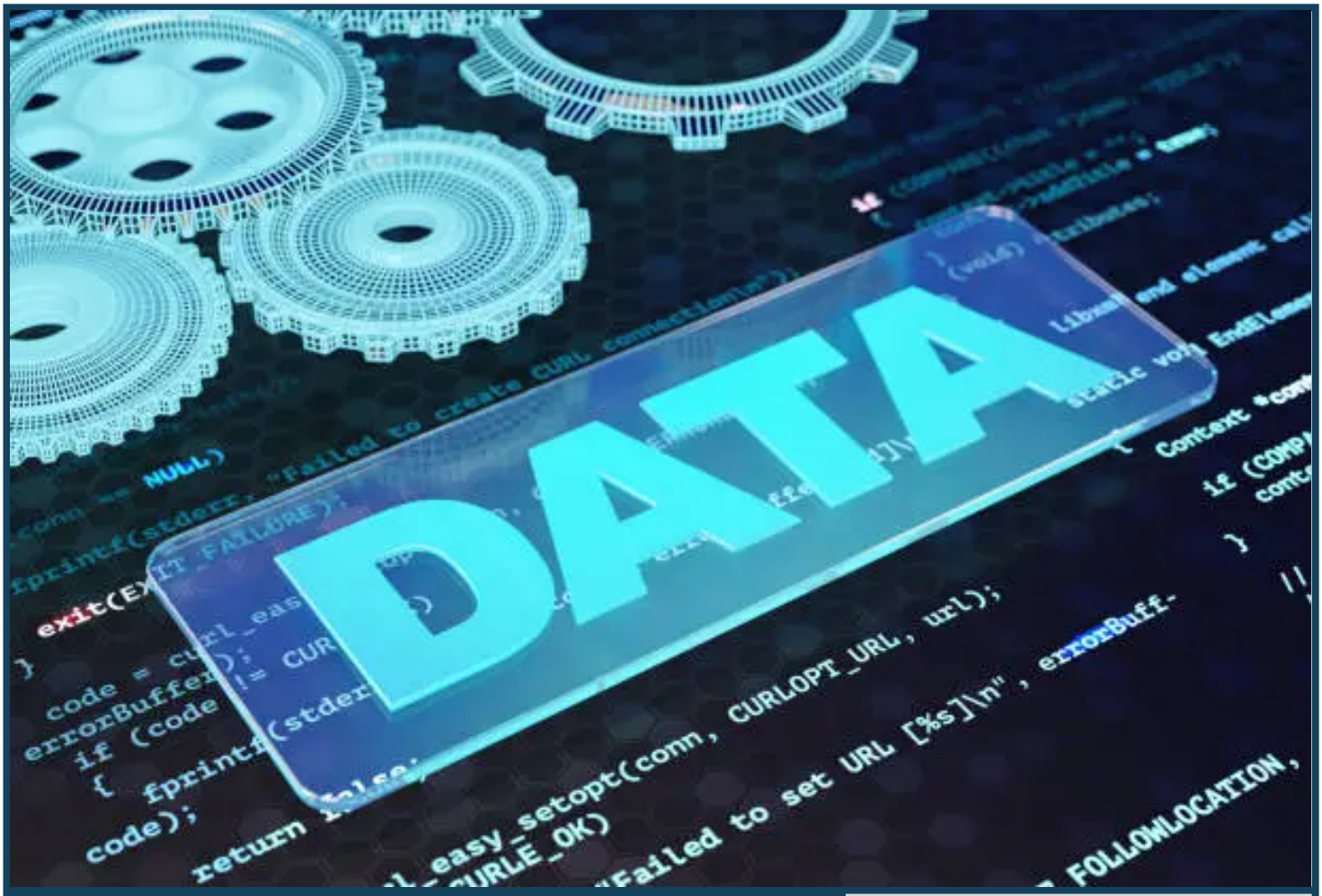
PUBLIC REPORT

INTERNAL AUDIT DEPARTMENT



Information Technology Audit:
OCIT
Data Governance Selected Controls
For the Year Ended December 31, 2025

Audit No. 2411
Report Date: September 17, 2026

Number of Recommendations

0	Critical Control Weaknesses
3	Significant Control Weaknesses
0	Control Findings

OC Board of Supervisors

CHAIR DOUG CHAFFEE	VICE CHAIR KATRINA FOLEY	SUPERVISOR JANET NGUYEN	SUPERVISOR VICENTE SARMIENTO	SUPERVISOR DONALD P. WAGNER
4th DISTRICT	5th DISTRICT	1st DISTRICT	2nd DISTRICT	3rd DISTRICT

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
OCIT Data Governance Selected Controls
September 17, 2026

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an audit of OC Information Technology (OCIT) to evaluate the effectiveness of the County's Data Governance Program, including policies, security controls, and compliance with Senate Bill (SB) 272 to provide reasonable assurance that data assets are managed effectively, securely, and ethically across departments for the year ended December 31, 2025.
RESULTS	Sensitive audit results have been removed from this report.
RISKS	Findings and related risks include: • The lack of a complete inventory of enterprise systems leads to visibility gaps, accountability failures, and elevated risk across the County. Also, failure to update the County's public enterprise systems catalog as required by SB 272, places the County in violation of state law, exposing it to potential legal and reputational risks. • Sensitive content for other findings has been removed from this report.
NUMBER OF RECOMMENDATIONS 0 CRITICAL CONTROL WEAKNESSES 3 SIGNIFICANT CONTROL WEAKNESSES 0 CONTROL FINDINGS	Opportunities for enhancing internal controls include: • OCIT implement formal processes and controls to regularly (e.g., annually) update their catalog of enterprise systems and the SB 272-mandated website. • Sensitive content for other findings has been removed from this report.

Report suspected fraud, or misuse of County resources by vendors, contractors, or County employees to (714) 834-3608

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2411

September 17, 2026

To: Ed Athlof
Interim Chief Information Officer

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Digitally signed by Aggie Alonso
Date: 2026.09.17 13:44:31 -07'00'

Subject: OCIT Data Governance Selected Controls Audit

We have completed an audit of the OC Information Technology (OCIT) Data Governance Program for the year ended December 31, 2025. Due to the sensitive nature of specific findings (restricted information), results are redacted from public release. Additional information including background, and our objectives, scope, and methodology are included in Appendix A.

OCIT concurred with all our recommendations, and the Internal Audit Department considers management's response appropriate to the recommendations in this report.

We will include the results of this audit in a future status report submitted quarterly to the Audit Oversight Committee and the Board of Supervisors. In addition, we will request your department complete a Customer Survey of Audit Services, which you will receive shortly after the distribution of our final report.

We appreciate the courtesy extended to us by OCIT during our audit. If you have any questions, please contact me at (714) 834-5442 or Deputy Director Jose Olivo at (714) 834-5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
KC Roestenberg, Interim County Executive Officer
OCIT Distribution
Robin Stieler, Clerk of the Board
Foreperson, Grand Jury
Crowe LLP, County External Auditor

INTERNAL AUDIT DEPARTMENT

RESULTS

BUSINESS PROCESS & INTERNAL CONTROL STRENGTHS	Business process and internal control strengths noted during our audit include: ✓ The Countywide Security Awareness Training completion rate for 2025 was greater than 90%. This training educates employees on cybersecurity threats and safe practices for securing their data. ✓ OC Information Technology (OCIT) conducts monthly Cybersecurity Joint Task Force meetings to discuss important cybersecurity matters, including data governance initiatives, such as working towards implementing a Countywide Data Governance policy. ✓ OCIT manages the Security Operations Center and provides after-hours, weekend, and holiday coverage to ensure 24/7 monitoring and response of abnormal activity on its network. ✓ OCIT has a Chief Information Security Officer and a Cyber Resilience Manager which help strengthen governance and accountability by aligning enterprise cybersecurity strategy, data governance, and operational resilience under clearly defined leadership roles.

FINDING NO. 1	Content has been removed due to sensitive nature of the specific findings.

FINDING NO. 2	Content has been removed due to sensitive nature of the specific findings.

FINDING NO. 3	**Compliance with California Senate Bill 272** California Senate Bill (SB) 272 requires local government agencies to create and regularly update a public catalog of their enterprise systems. Specifically, this includes multi-departmental systems or systems that contain information collected about the public, and systems must also serve as an original source of data within the agency. A systems catalog is also critical for OCIT to gain visibility into where data resides, who owns it, and how it is used, which is essential for data governance. We noted OCIT has a catalog of County enterprise systems. However, they do not have formal processes to regularly (e.g., annually) update the catalog or SB 272-mandated website. We also noted the catalog is incomplete, such as departments and their systems not listed at all, and OCIT indicated they have not updated the SB 272-mandated website in at least a year. OCIT indicated they are currently in the process of collecting updated system information from departments and will update the website as soon as possible.

INTERNAL AUDIT DEPARTMENT

CATEGORY	**Significant Control Weakness**
RISK	The lack of a complete inventory of enterprise systems leads to visibility gaps, accountability failures, and elevated risk across the organization. Also, failure to update the County's public catalog of enterprise systems as required by SB 272 places the County in violation of state law, exposing it to potential legal and reputational risks.
RECOMMENDATION	OCIT management implement formal processes and controls to regularly (e.g., annually) update their catalog of enterprise systems and the SB 272-mandated website to provide the foundation for effective data governance and risk management, and ensure compliance with State requirements.
MANAGEMENT RESPONSE	**Concur:** OCIT agrees with the finding that the information published on the SB 272 site is incomplete. It is important to note that data related to OCIT-managed systems for Shared and Managed Services agencies is updated annually. However, systems outside of OCIT's control are frequently omitted or outdated, primarily due to a lack of response from the responsible agencies. To remediate this issue, OCIT will implement the following processes: 1. OCIT will issue a formal memorandum to County department heads and information security officers annually by October 15, reminding them of the requirement to submit updated information by December 15. 2. If no response is received by December 1, OCIT will issue a second memorandum to the department head. 3. If an agency does not respond by the December 15 deadline, OCIT will issue a memorandum to both the department head and the County CEO. 4. All submitted records will be updated on the County SB 272 site by January 15 of the following year.

AUDIT TEAM	Jimmy Nguyen, CISA, CFE, CEH	Senior IT Audit Manager
	Michael Steinhaus, CISA, CIA, CPA	IT Audit Manager
	JC Lim, CIA, CISA, CFE	Administrative Services Manager

INTERNAL AUDIT DEPARTMENT

APPENDIX A: ADDITIONAL INFORMATION

OBJECTIVE	Evaluate the effectiveness of the OC Information Technology (OCIT) Data Governance Program, including policies, security controls, and compliance with Senate Bill (SB) 272 to provide reasonable assurance that data assets are managed effectively, securely, and ethically across departments.
SCOPE & METHODOLOGY	Our engagement scope will be for the year ended December 31, 2025 and will focus on OCIT's data governance program.
EXCLUSIONS	We did not evaluate application controls or processes that involve external parties such as Science Application International Corporations, the State of California, or third-party vendors.
PRIOR AUDIT COVERAGE	We have not issued any audit reports for OCIT with a similar scope within the last ten years.
BACKGROUND	The mission of OCIT is to deliver fiscally responsible, reliable, and secure technology solutions that empower the County to provide high-quality services to residents, visitors, and employees. A key part of this mission is ensuring appropriate governance over County data. Data Governance is a structured framework of policies, processes, roles, and standards designed to ensure data remains accurate, consistent, secure, and responsibly managed throughout its lifecycle. This is critical because the County depends on data to operate essential systems effectively. Robust data governance reduces risks such as breaches, inaccuracies, and compliance issues, while fostering accountability and trust in data-driven decision-making.

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the Fiscal Year 2025-26 Annual Risk Assessment & Audit Plan approved by the Board of Supervisors (Board).
PROFESSIONAL STANDARDS	Our audit was conducted in conformance with the Global Internal Audit Standards issued by the International Internal Audit Standards Board.
FOLLOW-UP PROCESS	In accordance with professional standards, the Internal Audit Department has a process to follow up on its recommendations. A first follow-up audit will generally begin six months after release of the initial report. The Audit Oversight Committee (AOC) and Board expect that audit recommendations will typically be implemented within six months or sooner for significant and higher risk issues. A second follow-up audit will generally begin six months after release of the first follow-up audit report, by which time all audit recommendations are expected to be implemented. Any audit recommendations not implemented after the second follow-up audit will be brought to the attention of the AOC at its next scheduled meeting. A Follow-Up Audit Report Form is attached and is required to be returned to the Internal Audit Department approximately six months from the date of this report to facilitate the follow-up audit process.
MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL	In accordance with the Auditor-Controller's County Accounting Manual No. S-2 Internal Control Systems: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls. Internal control should be continuously evaluated by management and weaknesses, when detected, must be promptly corrected." The criterion for evaluating internal control is the Committee of Sponsoring Organizations of the Treadway Commission Internal Control – Integrated Framework: 2013. Our audit complements but does not substitute for department management's continuing emphasis on control activities and monitoring of control risks.
INTERNAL CONTROL LIMITATIONS	Because of inherent limitations in any system of internal control, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the department's operating procedures, accounting practices, and compliance with County policy.

INTERNAL AUDIT DEPARTMENT

APPENDIX B: REPORT ITEM CLASSIFICATION

Critical Control Weakness	Significant Control Weakness	Control Finding
These are audit findings or a combination of audit findings that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise the department's or County's reputation for integrity. Management is expected to address **Critical Control Weaknesses** brought to its attention immediately.	These are audit findings or a combination of audit findings that represent a significant deficiency in the design or operation of internal controls. **Significant Control Weaknesses** require prompt corrective actions.	These are audit findings concerning the effectiveness of internal control, compliance issues, or efficiency issues that require management's corrective action to implement or enhance processes and internal control. **Control Findings** are expected to be addressed within our follow-up process of six months, but no later than twelve months.

APPENDIX C: OCIT MANAGEMENT RESPONSE

County Executive Office

Memorandum

August 27, 2026

To: Aggie Alonso, CPA, CIA, CRMA, Director, Internal Audit Department

From: Ed Althof, Interim Chief Information Officer

Subject: Audit No. 2411, OCIT Data Governance Controls Audit

Orange County Information Technology (OCIT) has received the draft report for the OCIT Data Governance Controls Audit. OCIT manage [redacted] environment, where most departments store their data on [redacted] Orange County Sheriff's Department (OCSD), Public Defender (PD), and District Attorney (DA) do not subscribe to the [redacted] and as such, maintain their own data. Furthermore, OCIT has developed and maintains the website for cataloging Enterprise Systems in accordance with California Senate Bill 272 for all County departments.

Please find OCIT's response to the audit findings and recommendations below.

Finding No. 1: [redacted]

[redacted]

Page 2

Category: [redacted]

Risk: [redacted]

Recommendation: OCIT management: [redacted]

OCIT Management Response: [redacted]

The CEO's Office Response: [redacted]

[redacted]

Finding No. 2: [redacted]

[redacted]

Category: [redacted]

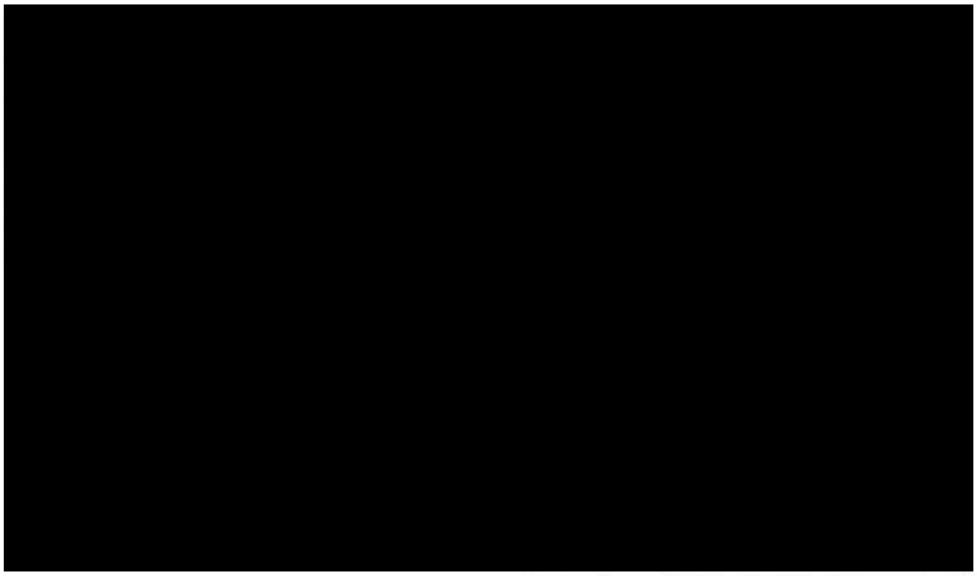
Risk: [redacted]

Recommendations: OCIT Management:

[redacted]

OCIT Management Response:

Page 4



Finding No. 3: Compliance with California Senate Bill 272

California Senate Bill (SB) 272 requires local government agencies to create and regularly update a public catalog of their enterprise systems. Specifically, this includes multi-departmental systems or systems that contain information collected about the public, and systems must also serve as an original source of data within the agency. A systems catalog is also critical for OCIT to gain visibility into where data resides, who owns it, and how it is used, which is essential for data governance.

We noted OCIT has a catalog of County enterprise systems. However, they do not have formal processes to regularly (e.g., annually) update the catalog or SB 272-mandated website. We also noted the catalog is incomplete, such as departments and their systems not listed at all, and OCIT indicated they have not updated the SB 272-mandated website in at least a year.

OCIT indicated they are currently in the process of collecting updated system information from departments and will update the website as soon as possible.

Category: Significant Control Weakness

Risk: The lack of a complete inventory of enterprise systems leads to visibility gaps, accountability failures, and elevated risk across the organization. Also, failure to update the County's public catalog of enterprise systems as required by SB 272 places the County in violation of state law, exposing it to potential legal and reputational risks.

Recommendations: OCIT management implement formal processes and controls to regularly (e.g., annually) update their catalog of enterprise systems and the SB 272-mandated website to provide the foundation for effective data governance and risk management, and ensure compliance with State requirements.

OCIT Management Response:

OCIT agrees with the finding that the information published on the SB 272 site is incomplete. It is important to note that data related to OCIT-managed systems for Shared and Managed Services agencies is updated annually. However, systems outside of OCIT's control are frequently omitted or outdated, primarily due to a lack of response from the responsible agencies.

To remediate this issue, OCIT will implement the following processes:

1- OCIT will issue a formal memorandum to County department heads and information security officers annually by October 15, reminding them of the requirement to submit updated information by December 15.
2- If no response is received by December 1, OCIT will issue a second memorandum to the department head.
3- If an agency does not respond by December 15 deadline, OCIT will issue a memorandum to both the department head and the County CEO.
4- All submitted records will be updated on the County SB 272 site by January 15 of the following year.

cc: KC Roestenberg, Interim County Executive Officer
Andrew Alipanah, Chief Information Security Officer
Jose Tostado, Director, Strategy, Innovation and Architecture – OCIT
Ray O'Grady, Director, Data Center Services – OCIT
Jayesh Patel, Director, E-Gov Software & Applications – OCIT
Thuy Vu-Le, Director, Administrative Services – OCIT