Performance Audit of the San Diego Convention Center's Financial Systems

FINANCIAL SYSTEM ACCESS CONTROLS FOR PRIVILEGED USERS REQUIRE IMPROVEMENT

MAY 2014

Audit Report
Office of the City Auditor
City of San Diego

OCA
Independent • Objective • Accurate

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

THE CITY OF SAN DIEGO

May 30, 2014

Carol Wallace, President and Chief Executive Officer
San Diego Convention Center

Transmitted herewith is an audit report on the San Diego Convention Center's Financial Systems. We have completed this report as requested by the Convention Center. This report is presented in accordance with City Charter Section 39.2. Management's response to the report is presented on page 17.

We would like to thank the Convention Center's staff for their assistance and cooperation during this audit. All of their valuable time and efforts spent providing us information is greatly appreciated. The audit staff members responsible for this audit report are Stephen Gomez, Danielle Knighten, and Kyle Elser.

Respectfully submitted,

Eduardo Luna

Eduardo Luna
City Auditor

cc: City of San Diego Audit Committee Members

Results in Brief

The San Diego Convention Center (SDCC) Facilitates events in the San Diego region creating economic benefit for the region as a whole with a midsized corporation staff. The SDCC reports their audited annual financial statements to the general public and investors based on the financial data recorded and processed in their financial systems.

We found that their financial system do not have controls in place to mitigate users with privileged access from damaging the financial systems. Specifically, the privileged access could be used to:

1) Modify the Convention Center's financials over time without identification;

2) Destroy or Corrupt the Convention Center's electronic financial records and data;

3) Make unauthorized payments from the system.

The high level of privileged access exists because it is required to maintain, upgrade, and repair the system when problems arise.

The San Diego Convention Center Corporation has a relatively small staff; several of whom have been there for over 10 years. As a result, the personnel who know the system very thoroughly and have been there for many years are the ones that can maintain it when issues, questions, or upgrades occur. These users are granted the access to perform these roles and are in higher positions in the office partly due to their reliability, knowledge, and time spent at the corporation.

While these people are the most knowledgeable and best able to provide these services to keep operations running smoothly, they also present the largest risk as they have no one above them who have the ability to review their activities at the detail required to identify inappropriate activities.

The Convention Center can follow standard IT control guidelines provided by ISACA to mitigate these risks while still allowing the knowledgeable users the access they need to maintain the systems when the need arises.

Background

The San Diego Convention Center's Role in San Diego

The San Diego Convention Center (SDCC) facilitates business, educational, social, cultural, and entertainment activities through several types of events, including convention and trade shows, consumer shows, conferences, community functions, meetings, seminars and performing arts. SDCC is a nonprofit public benefit corporation founded in 1984 by the City of San Diego, and operates under an independent Board of Directors appointed by the San Diego City Council.

SDCC's Economic Impact to the San Diego Region

According to their 2013 annual report, the Convention Center generated $1.3 billion in economic impact to the San Diego region resulting from 148 events held in the building and the more than 760,000 attendees associated with those events. In addition to the significant economic benefits, an estimated 12,500 local jobs are supported by events held at the center.

The SDCC projects their total operating revenues to be approximately $33.2 million dollars for Fiscal Year 2014. Due to the nature of their business, they schedule events far in advance, with several repeat annual events such as Comic-Con. In addition, the SDCC collects full payment prior to each event. The advance planning and collection of fees allows for a detailed revenue projection.

SDCC Current and Previous IT Performance Audits

The San Diego City Auditor's Office (OCA) previously conducted a performance audit of the San Diego Convention Center's (SDCC) information technology network infrastructure in 2012 at the request of the Convention Center. The Audit of the SDCC's IT Infrastructure was the first of four IT risk areas identified in a previous risk assessment of the organization information systems environment as shown below:

1. IT infrastructure operations and security;
2. Financial systems IT controls;
3. Human Resources contracted system services; and
4. Management of IT system implementations; specifically, the implementation of the customer relationship management system.

The purpose of the infrastructure audit was to identify security and operational risks to SDCC's IT infrastructure prior to assessing the risk of the systems that relied on the infrastructure, such as the Financial Systems.

Our audit of the infrastructure did not identify any significant risks at the infrastructure level; however, the audit did suggest that the Convention Center make improvements to the IT Security Governance documentation, Network activity logging, and implement additional segregation of duties among IT functions.

The SDCC's management response letter informed us that they had implemented the improvements, with the exception of improved logging as they believed the default settings met their requirements. Our current audit of the Financial Systems IT Controls builds on the audit work performed during the IT Infrastructure audit.

Through our risk assessment described in **Appendix B**, we identified two primary systems within the process and two secondary systems. The primary systems were Microsoft Dynamics SL, which is used to track the overall financial activities for the Convention Center. The second was ConCentRICs, which is used to track the Convention Center event revenue at a detailed level. The Data is then rolled up into Microsoft Dynamics SL through manual data entry and monthly reconciliation of independent system GL accounts. The two secondary systems were Microsoft Dynamics Customer Relationship Management (CRM) which is used to track customer contracts, and Sage Asset Management which manages and tracks depreciation of SDCC assets above a $5,000 threshold.

Audit Results

Finding 1: FINANCIAL SYSTEM ACCESS CONTROLS FOR PRIVILEGED USERS REQUIRE IMPROVEMENT

The Convention Center's Financial System IT Controls over privileged users[1] are inadequate to detect or prevent significant harm to the financial systems and their corresponding data. Specifically, the privileged access could be used to:

1) Modify the Convention Center's financials over time without identification;
2) Destroy or Corrupt the Convention Center's electronic financial records and data;
3) Make unauthorized payments from the system.

Privileged Access Granted to Financial Systems without Mitigating Controls

During our audit risk assessment we identified four systems that support and automate the financial processes. These systems all contain users with unmitigated privileged access to sensitive portions of the financial data throughout the process which presents a significant risk to the financial records.

The four systems identified as in-scope for the audit of the Financial Systems are shown in <u>**Exhibit 1**</u> below. These systems house the core financial data used to report their audited annual financial statements used to determine the financial health and manage financial operations for the San Diego Convention Center.

[1] A privileged user is a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

Exhibit 1: Convention Center Financial Systems

System Name	System Process Function
Microsoft Dynamics SL	Core Financial/Accounting System
ConCentRICs	Detailed Event Accounts Receivables
Microsoft Dynamics CRM	Customer Relationship Management System
SAGE Asset Management	Fixed Asset Management System

Source: Auditor Generated Based on SDCC Data

During our audit, we found that several users have access to privileged accounts in the Financial Systems. These users are primarily the IT Staff up to the director level, with the addition of the Accounting Director and a contracted system support specialist for Microsoft Dynamics SL.

The Accounting Director also acts as Administrator in the Convention Center's core financial system (Microsoft Dynamics SL), the Asset Management System (SAGE), and portions of the event revenue accounting system (ConCentRICs). In addition, the Accounting Director has Accounting, Procurement, and Sales account access to the Customer Relationship Management (Microsoft Dynamics CRM) system used to initiate the event revenue stream.

The IT Director has Administrative Access to all systems with the exception of the Asset Management System, but most likely has the ability to administer the system owing to his position. The IT Staff utilize the generic Administrator accounts to access and administer the financial systems.

Based on our review, there are no active reviews of activities within the financial systems to compensate for the privileged access in use. In addition, the primary Financial system does not have the native ability to log an individual user's activity in the system. However, there are commercially available tools and customizations to perform this function.

Unmitigated Privileged Access Presents a Significant Risk to SDCC's Financial Data

The privileged and system administration access available to several users allow them to perform any activity allowed in the Microsoft Dynamics SL and key functions in the remaining financial systems without mitigation. With sufficient knowledge of the Convention Center's business processes this access could be used to:

1) Modify the Convention Center's financials over time without identification;
2) Destroy or Corrupt the Convention Center's electronic financial records and data;
3) Make unauthorized payments from the system.

In addition, some of the users with access also oversee the back-up of the data, giving the potential of destroying any ability to restore damaged financial data[2].

The Need for Privileged Access

The high level of privileged access exists because it is required to maintain, upgrade, and repair the system when problems arise.

The San Diego Convention Center Corporation is a midsized corporation, with a relatively small staff; several of whom have been there for over 10 years. In addition, the personnel who know the system very thoroughly and have been there for many years are the ones that can maintain it when there are issues, questions, or upgrades. These users are granted the access to perform these roles and are in higher positions in the office partly due to their reliability, knowledge, and time spent at the corporation.

While these people are the most knowledgeable and best able to provide these services to keep operations running smoothly, they also present the largest risk as they have no one above them who have the ability to review their activities at the detail required to identify inappropriate activities.

[2] The IT Director oversees IT Operations, including the back-up of financial systems and data

Best Practice for a Controlled Systems Environment

To mitigate these risks, an international organization, ISACA, provides standards for information system controls designed to prevent misuse and protect information system resources.

The Convention Center can apply ISACA's control guidance to protect their information resources including the financial systems reviewed in this audit. The following controls are excerpts that apply to the SDCC Financial Systems Environment from ISACA's control documentation. To mitigate these risks, ISACA specifies that[3]:

Preventative Controls 2.16.1

- Procedures should exist to define, approve process, revoke, eliminate, change, communicate, log and audit access, approved by owners and supervisors.
- User administration procedures, including daily controls over the administration function should be in place.
- Application of segregation of duties—dividing access to critical data between two or more persons to reach a level of mutual control

Detective Controls 2.17.1

- Activities of the privileged or super user login account should be closely monitored and reviewed by senior computer security management.
- Audit/quality assurance reviews of entitlements, high-privilege users, functional users, default users, special groups/roles, firewall/Intrusion Detection Systems (IDS) configurations, alerts and logs should be in place.
- The logs containing non-approved activities should be logged and reviewed.

[3] Referenced controls are excerpts from ISACA's G38 Access Controls Guideline document, based on COBIT's control framework. COBIT was formerly known as the Control Objectives for Information and Related Technology, and now is simply COBIT.

Controls Over Information Security Administration (ISA) 2.20.1

- All ISA activities should be recorded in audit logs.
- All user administration functions should be segregated from any other activities (i.e., system administration, business transactions and developer activity); otherwise, inappropriate segregation of duties will lead to conflicts of interest.
- One independent party should control all ISA activities in 24 hours or should implement maker/checker dual control to verify that only required actions are processed.
- All privileged users (administrators, Database Administrators) should be monitored and have a tighter control process for justification, documentation and approval.

Controls over user activities 2.22.1

- Access to critical accounts, log files, data files and databases should be monitored.
- Periodically, logs should be reviewed to monitor activities of privileged users and failed access attempts

Methods to Apply Information Systems Controls to SDCC's Financial Systems Environment

One effective method to employ these controls and mitigate the risks includes removing privileged access from the user accounts and creating a "firefighter account" that includes privileged access. This account would need to be secured and only used when necessary, and would log any user of the account and all the activities performed while the account was in use. The activity would then be reviewed by a responsible party knowledgeable about the system, who would sign off on the authorized activity and lock the account until it is needed again.

Typically, the party responsible for the account would be the IT Director; however, the responsible party would also have to give up any privileged access to the system to ensure separation of duty conflicts do not occur – as it would not be a strong control for the IT Director to review his own modifications in the financial systems.

Another level of security could be to require an automated notification to an appropriate user or group of users whenever these privileged accounts are used, and by whom. This notification would alert a reviewer that the account has been used, and would precipitate a review of the activity to confirm it was approved.

Recommendation #1 **The San Diego Convention Center should mitigate the privileged system access to ensure controls prevent one user from damaging or inappropriately modifying financial data. Specifically,**

a) All privileged access should be removed from the general user accounts.

b) Privileged accounts should be secured from general access and only used when necessary with an appropriate approval process.

c) Users should be identified and tracked when using a privileged account.

d) All activities performed while the privileged account is in use should be recorded and reviewed by someone who did not access the account during the session under review, but knowledgeable enough to understand the logged activity.

e) Responsibility to maintain the back-ups of financial systems and data should be segregated from users of the financial privileged access to prevent one person from destroying the data and wiping out the back-ups of that data (Priority Level 1).

Recommendation #2 **The San Diego Convention Center should document their mitigation strategy and ensure that their approach mitigates access across the financial systems and back-ups of financial systems and data, and detail the procedures used to implement their strategy on a day to day bases. This Strategy must incorporate the provisions defined in Recommendation 1 (Priority Level 2).**

Conclusion

The San Diego Convention Center (SDCC) Facilitates events in the San Diego region creating economic benefit for the region as a whole with a midsized corporation staff. The SDCC reports their audited annual financial statements to the general public and investors based on the financial data recorded and processed in their financial systems.

We found that their financial system does not have controls in place to mitigate users with privileged access from damaging the financial systems and we made two recommendations to mitigate these risks. The SDCC agreed to implement the recommendations which they plan to complete by the end of July 2014.

Appendix A: Definition of Audit Recommendation Priorities

DEFINITIONS OF PRIORITY 1, 2, AND 3 AUDIT RECOMMENDATIONS

The Office of the City Auditor maintains a classification scheme applicable to audit recommendations and the appropriate corrective actions as follows:

Priority Class[4]	Description[5]	Implementation Action[6]
1	Fraud or serious violations are being committed, significant fiscal or equivalent non-fiscal losses are occurring.	Immediate
2	A potential for incurring significant or equivalent fiscal and/or non-fiscal losses exist.	Six months
3	Operation or administrative process will be improved.	Six months to one year

[4] The City Auditor is responsible for assigning audit recommendation priority class numbers. A recommendation which clearly fits the description for more than one priority class shall be assigned the higher number.

[5] For an audit recommendation to be considered related to a significant fiscal loss, it will usually be necessary for an actual loss of $50,000 or more to be involved or for a potential loss (including unrealized revenue increases) of $100,000 to be involved. Equivalent non-fiscal losses would include, but not be limited to, omission or commission of acts by or on behalf of the City which would be likely to expose the City to adverse criticism in the eyes of its residents.

[6] The implementation time frame indicated for each priority class is intended as a guideline for establishing implementation target dates. While prioritizing recommendations is the responsibility of the City Auditor, determining implementation dates is the responsibility of the City Administration.

Appendix B: Objectives, Scope, and Methodology

Objectives

In accordance with the City Auditor's FY 2014 Work Plan and at the request of the San Diego Convention Center (SDCC), we conducted an IT audit of the Financial Systems to assess the strength of the access and monitoring controls over the financial systems and corresponding reporting ability.

Specifically, our objective was to identify areas with weak controls in the financial systems, including identifying users with excessive or uncontrolled access, methods of circumventing access restrictions, and confirm targeted monitoring of high risk areas within the system.

Scope & Methodology

In order to ensure we reviewed all relevant financial information systems corresponding to the financial processes, we performed a risk assessment of SDCC's financial systems environment, including a review of SDCC's financial business processes.

Through this assessment we identified two primary systems within the process and two secondary systems. The primary systems were Microsoft Dynamics SL, which is used to track the overall financial activities for the Convention Center. The second was ConCentRICs, which is used to track the Convention Center event revenue at a detailed level. The Data is then rolled up into Microsoft Dynamics SL through manual data entry and monthly reconciliation of independent system GL accounts. The two secondary systems were Microsoft Dynamics Customer Relationship Management (CRM) and Sage Asset Management.

We then analyzed the application security environment of these financial systems, which built on our previous audit of SDCC's general IT Infrastructure control environment.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

San Diego
Convention Center
Corporation

WWW.VISITSANDIEGO.COM
111 WEST HARBOR DRIVE, SAN DIEGO, CA 92101
PHONE 619.525.5000 • FAX 619.525.5005

May 29, 2014

Mr. Eduardo Luna
City Auditor
Office of the City Auditor

Dear Mr. Luna:

The San Diego Convention Center Corporation's management would like to thank the City Auditors for their through audit of our Financial Management IT Controls. The following summarizes the recommendations contained in this report and Management's response

Recommendation #1: The San Diego Convention Center should mitigate the privileged system access to ensure controls prevent one user from damaging or inappropriately modifying financial data. Specifically,

a) All privileged access should be removed from the general user accounts.
b) Privileged accounts should be secured from general access and only used when necessary with an appropriate approval process.
c) Users should be identified and tracked when using a privileged account.
d) All activities performed while the privileged account is in use should be recorded and reviewed by someone who did not access the account during the session under review, but knowledgeable enough to understand the logged activity.
e) Responsibility to maintain the back-ups of financial systems and data should be segregated from users of the financial privileged access to prevent one person from destroying the data and wiping out the back-ups of that data (Priority Level 1).

Management Response: Agree

Recommendation #2: The San Diego Convention Center should document their mitigation strategy and ensure that their approach mitigates access across the financial systems and back-ups of financial systems and data, and detail the procedures used to implement their strategy on a day to day bases. This Strategy must incorporate the provisions defined in Recommendation 1 (Priority Level 2).

Management Response: Agree

The expected date of completion of the implementation of recommendations is July 2014.

Tom Mazzocco
Executive Vice President & COO