



Smart decisions. Lasting value.™

CITY OF CORAL GABLES, FLORIDA

Internal Audit of User Access Controls

November 2017

Distribution:
Mayor and City
Commissioners



TABLE OF CONTENTS

	<i>Page</i>
EXECUTIVE SUMMARY	
Overview.....	1
Summary of Results.....	1
INTRODUCTION	
Scope.....	2
Risk Management.....	3
OBSERVATION AND RECOMMENDATION.....	4

EXECUTIVE SUMMARY

Overview

Crowe Horwath LLP (“Crowe” or “we”) performed internal audit procedures related to the City of Coral Gables’ user access control functions. The objectives of the audit were to evaluate policies and procedures over user access control and establishing whether controls were adequate to actively monitor access in the selected departments.

Summary of Results

The following is a summary of our observations as a result of our procedures. We listed the opportunity for improvement and corresponding risk rating. Additional information can be found on page 4 of this report.

Opportunity for Improvement	Audit Finding	Risk Rating**
1	Segregation of Duties	Moderate

**For explanation of *Risk Rating* determination, refer to page 3.

INTRODUCTION

Background

The City's Information Technology Policy states that all City staff and users share the responsibility of protecting the Information Resources for which they have access and/or ownership. The department directors are primarily responsible for particular data/information systems and they determine who is authorized to access these resources.

Scope

The scope of this audit included the following:

- Selection and testing of a sample of EDEN users from the Finance, IT, HR and Payroll departments and evaluation of user permissions in the system.
- Selection and testing of EDEN users and testing that their role was properly classified in the system and they were current City employees.
- Review of policies and procedures and other supporting documentation provided by the City.

INTRODUCTION

Risk Management

As part of our procedures, we conducted a risk assessment for each process in the scope of our performance audit. As part of this risk assessment, we analyzed the risks, internal controls and gaps that existed in each process.

Risks are evaluated based on its “significance” to management’s strategy and its “likelihood” to occur. This will result in a risk profile of the highest risks to the organization as presented below:



OBSERVATION AND RECOMMENDATION

1. **OPPORTUNITY FOR IMPROVEMENT – Segregation of Duties: MODERATE RISK**

From a listing of 384 Eden users, we selected 25 users for testing. During our testing of user access roles, we found that two employees had full permission access to modules that did not appear to be necessary for their respective job duties.

Recommendation: An overall review of permissions needs to be performed to correct and update EDEN access controls. In addition, there should be a periodic review of EDEN access permissions to ensure that users and access permissions are authorized, remain appropriate and provide an appropriate level of segregation of duties.

Management Response / Action Plan:

The Information Technology department will work with the Finance Department’s leadership reviewing the two identified user accounts where it was found that segregation of duties needs to be improved. I.T. and Finance will perform the necessary corrections as per auditor’s recommendations and further review. The review and correction of the two user accounts will be completed by end of November 2017.

The Information Technology department is performing an overall review of permissions in EDEN with Finance and all city departments. Access controls are being updated according to that review with department heads, and per auditors’ recommendations. This review will be completed by end of December 2017.

This citywide review of user permissions in EDEN is scheduled annually as part of the I.T. Department’s operation plan (CGITOP), as annual recurring task CGITOP-A-15: “Comprehensive access review of all EDEN users - IT & Department heads.” Description: “Required by auditors: once a year review access in EDEN of all city users, verify with department heads.” This annual access review requirement is currently being audited also by the external auditor firm RSM McGladrey.