Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Audit Team on the Engagement:
Jacob Claeys, CGAP, CICA
Magdy Mossaad, MBA, CIA, CMA, CFE, CPA
Protiviti

- Mike Thor
- David Lubin
- Benny Sharp
- Marc Doyle
- Paul Slye

Database Access Review

Published by Order of the Audit Committee
on
April 25, 2012

Report # 2012-03

This Database Access Review included a review of security data that the Minnesota Data Practices Act legally classifies as not public. To protect City resources and comply with the Act, we withheld specific security-related details from this publicly released report. We communicated all pertinent details to management in a separate, not public document.

Date: April 25, 2012

To: Otto Doll, Information Technology (IT)

Cc: Beth Cousins, IT
Jayne Khalifa, City Coordinator's Office
Deb Parker, IT
Bert Sletten, IT

Re: Database Access Review Report # 2012-03

Background

The City of Minneapolis (The City) processes and retains information on behalf of citizens, employees and other stakeholders that is classified as not public data by the Minnesota Government Data Practices Act. The City has legal requirements under state and federal law to safeguard the not public data it retains. Effective information security relies on the combination of robust technical configurations, automated and/or manual processes and proper, accountable and/or appropriate human behavior to ensure the confidentiality, integrity, and availability of corporate systems and data.

The Internal Audit Department (IA) engaged Protiviti Inc. (Protiviti)[1] to perform a database access review. This report is intended solely for the use of management and leadership of the City and is not to be used or relied upon by others for any purpose whatsoever. This report and the related findings and recommendations detailed herein provide management with information about the condition or risks and internal controls at a point in time. Future changes in environmental factors and actions by personnel may adversely impact or enhance these risks and controls in ways that this report did not and cannot anticipate. For all responses where management is not choosing to follow the recommendations, the City is accepting the associated risk.

This report presents the results of the Database Access Review that was performed for the City during November and December 2011. The scope of the review was limited to specific database management system software and controls around access to databases using this software. This executive summary report is designed for the reader to understand the level of access assessed, to identify deficiencies and areas of strength and weakness, and to develop a course of action to correct improper access and mitigate associated risks.

Additionally, this report contains information concerning potential vulnerabilities related to access to City databases. This Database Access Review included a review of security data that the Minnesota Data Practices Act legally classifies as not public. To protect City resources and comply with the Act, IA withheld specific security-related details from this publicly released report. IA communicated all pertinent details to management in a separate, not public document.

Objectives and Scope

The primary objective of the review was to identify and evaluate controls around access to the database instances supporting PeopleSoft modules at the City. Specifically, this project focused on determining whether controls including processes, procedures and configurations are adequately designed and implemented to provide reasonable protection against unauthorized access. During the review, the principle of least privilege was used to evaluate appropriate access, where the minimal level of access required to perform job functions is all that a user should have. Fieldwork was conducted from November 14, 2011 through December 20, 2011.

[1] Any reference to Internal Audit throughout this report refers to the work performed by Protiviti.

A sample of ten (out of 15 total) databases was selected for review from a list of City systems considered to be higher risk because they contain not public data and/or perform critical data processing functions.

The scope of the review included the following:

- Review how authentication and access controls are implemented and restrict access.
- Review the account management process including user approval, maintenance and removal.
- Verify that an account review process has been implemented.
- Review system administrator access to database servers.

Summary of Conclusions

The City has controls that need improvement to help ensure access to the not public data stored is limited to those individuals who need assigned privileges. Despite this, some security measures that provide reasonable protection are being followed currently. Secure methods for authentication are used for accessing the databases and systems. Logging and monitoring is used to ensure that security related events are captured and reviewed. Currently identified users are assigned roles that are appropriate to what their job function is.

Areas needing improvement observed during the review include the following: documentation surrounding account management is incomplete. The currently followed process is unclear to all users and administrators, which results in actions and decisions that are not in accordance with policy nor secure. The City shares responsibility for administering the database systems with the managed services provider, and there is not a clear communication path between the two organizations in performing this administration. Review of user accounts and access privileges does not occur on a regular basis. Accounts are shared, which makes it difficult to know the identity of all users who have access to the account. Additionally, password management is difficult with shared accounts as constant password rotation is needed to remove access from users who no longer need it.

IA has provided in this report several recommendations for improving database access control policies, procedures and practices to the management of the IT Department. There are short term solutions to the current state of access that included performing a review of accounts and taking steps to ensure that proper access is granted. Additionally, with two organizations granting access to systems and databases, clear policies and procedures need to be setup in the long term that meet the business needs of the City and are agreed upon by both parties. These should clearly define who approves access related requests, how accounts are requested and created, what roles can be assigned to users, how and when to remove accounts, how to modify an account's privileges and when to conduct periodic reviews. Once in place, these can be communicated and enforced to produce a closed-loop process. Accounts should be tied to individuals and central systems should be in place to know what accounts are assigned to each individual. All of these security elements combined will enhance database security and controls.

Criticality Rating Definitions

IA has assigned one of the following risk levels to the observations made during this assessment. Each risk level indicates the impact and likelihood of observed vulnerabilities in the City's control environment. This assessment can be used by management as a tool to determine how quickly attention should be given to each observation provided within this report. Risk levels assignments are subjective and based on the scope of work completed for this assessment only.

The risk levels assigned by internal audit are described below:

Risk Level	Significance
High	Observed vulnerabilities assigned a high risk level are considered to present an imminent and significant threat and should be addressed as soon as possible.
Medium	Observed vulnerabilities assigned a medium risk level do not pose an immediate threat, but could likely cause a noticeable impact. These should be addressed in a timely manner once high level risks have been addressed.
Low	Observed vulnerabilities assigned a low risk level are considered to present threats that are unlikely to occur and would have a smaller impact. These should receive the lowest priority when being addressed.

Summary of Observed Vulnerabilities

The table below provides a summary of the observations identified during the 2011 database access review.

Ref.	Observed Vulnerability	Criticality
Database Access Review		
1.1	**Incomplete Policy and Procedure Documentation** Documentation for managing access to databases and systems is currently incomplete. *IT Management agrees and will implement solutions to address this issue by December 31, 2012.*	Medium
1.2	**Lack of Formalized Account Management Process** The current policies and procedures in place at the City have not been formalized regarding the process that is followed for access to databases and systems. *IT Management agrees and will implement solutions to address this issue by December 31, 2012.*	Medium
1.3	**Shared and Unknown Database Accounts** Four shared accounts and seven accounts with unknown uses were identified with varying privileges to the database management software. The external IT vendor currently has password management policies for shared accounts to help mitigate this risk, but the degree to which these policies are followed was not observed to be consistent for all shared accounts. *IT Management agrees and will implement solutions to address this issue by December 31, 2012.*	Medium

Abbreviations / Definitions Used Throughout the Report	
The City	City of Minneapolis
IA	Internal Audit Department
Shared Accounts	Single user accounts used by multiple individuals through a shared user name and password.