

Clause embodied in Report No. 2 of the Audit Committee, as adopted by the Council of the City of Toronto at its meeting held on March 1, 2 and 3, 2004.

6

Oracle Database Review – Security Controls and Other Issues

(City Council on March 1, 2 and 3, 2004, adopted this Clause, without amendment.)

The Audit Committee recommends the adoption of the report (December 12, 2003) from the Auditor General:

Purpose:

To review security controls relating to the City's Oracle databases managed by the Information & Technology Division of the Corporate Services Department.

Financial Implications and Impact Statement:

There are no immediate financial implications resulting from the adoption of this report. However, the adoption of the recommendations contained in this report will improve internal security controls. The adoption of the recommendations in our view can be accommodated with existing resources.

Recommendations:

It is recommended that:

- (1) City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and report to the July 2004 meeting of Audit Committee on the results of their reviews including any action taken;
- (2) the Commissioner of Corporate Services, direct that a self-assessment security audit be conducted on all major computer applications directly supported by the Information & Technology Division. In conducting this audit, consideration be given to the audit steps contained in various publications including the publication of the United States General Accounting Office entitled "Federal Information System Controls Audit Manual" and the publication entitled "Oracle Security Step-by-Step: A Survival Guide for Oracle Security." Copies of all such self-assessment audit reports be forwarded to the Auditor General's Office for review, evaluation and subsequent audit;

- (3) the Commissioner of Corporate Services, provide a written response to the Audit Report dated January 26, 2001, entitled "Information Security Framework" and forward such report to the July 13, 2004 meeting of the Audit Committee. The report from the Commissioner should include an update on the action taken on the recommendations included in the report dated January 26, 2001;
- (4) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report to the City's Administration Committee on the benefits and costs of establishing a centralized database security function with authority to administer and monitor database security practices for all databases throughout the City;
- (5) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, prepare a City-wide protocol and process for the development, approval, implementation and communication of all new or revised information technology policies and procedures. In addition, the Commissioner of Corporate Services, finalize the "Oracle Database Standards and Procedures" document ensuring it adequately addresses Oracle security;
- (6) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the current practices in connection with the installation of software patches to Oracle and other software applications. Such a review ensure that:
 - (a) an analysis is done to ensure that the benefits of installing specific software patches outweigh the risk and costs inherent in not applying the software patches;
 - (b) a process be implemented in order to ensure that information in regard to software patches is disseminated throughout the City; and
 - (c) patches, where required, have been appropriately and consistently installed.
- (7) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the extent to which Oracle's standard auditing features should be activated and this process be implemented corporate wide. Any decisions in relation to the activation or otherwise should be documented and approved by supervisory staff. As a minimum, we recommend the logging and timely review of unsuccessful access attempts;
- (8) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, direct database administrators throughout the City to review all passwords for default accounts provided by the Oracle Corporation in order to ensure that all such default passwords have been changed. Passwords be changed where appropriate;
- (9) the Commissioner of Corporate Services update, document and test the database business continuity plan for the databases administered by the Information & Technology Division and such documentation be centrally maintained;
- (10) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, take the necessary steps to centralize, within the City's Information & Technology Division, the custody, recording and administration of all Oracle database software licenses for the City; and

- (11) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.

Background:

The City of Toronto, in providing its many services to the public generates a significant amount of data. For example:

- the Tax and Water billing system in the Finance Department contains information concerning property assessments, names and addresses of taxpayers, meter reading information and tax and water billings, both current and historical;
- the registration system in the Parks and Recreation Division contains information on parks and recreation programs, residents addresses and registration to various programmes as well as a wide range of financial information;
- the Toronto Maintenance Management System contains information relating to repairs to City roads;
- the City's SAP financial system contains financial, payroll and human resource information, much of which is personal in nature;
- the Board of Health operates a system which contains significant information relating to the inspections of food premises; and
- the parking tag information system contains details relating to many thousands of parking tag infractions including vehicle license numbers and addresses of those citizens to whom parking tickets were issued.

While the cost of the computer equipment relating to the storage of this data is significant, the data itself is by far the more valuable asset of the City. Ensuring the adequacy of security to protect this asset is extremely important.

The amount of data collected by the City would be extremely difficult to manage without the use of a computer system and related computer software. To organize the data and make it useful it is stored in what are known as databases. The two major software databases currently in use at the City are Oracle and DB2. Oracle software is by far the most prevalent database software in use at the City.

The security of the various databases at the City is of paramount importance. Once the data is organized and stored in these databases, it is critical to ensure that it is protected from unauthorized changes or access. Privacy legislation also requires that the data be secure and protected from unauthorized disclosure. Failure to properly protect the data could have serious consequences for the City such as the potential for lost revenue from tax, water billings and parking infractions as well as the possibility for legal liability for the non protection of personal and private information to third parties. Also, if data is intentionally or unintentionally altered significant resources would be required to restore the changed data.

In addition, just as there are many databases, there are many networks throughout the City. Often staff need to access data on more than one network which means there are interconnections between these networks. Because of the number of interconnections that are required, virtually every computer could, in the absence of security controls, gain access to any other computer. These connections extend to the Internet, which connects the City's computer networks to any computer with access to the Internet. It is possible therefore, that anyone, from any location, with access to the Internet could in the absence of security controls access all data at the City. More seriously, once such access was gained, the person could change or delete the data.

Scope and Objectives of the Review

A significant part of the City's data resides on Oracle databases. This report focuses on the security over those databases. Other databases exist at the City, such as DB2 at the Toronto Police Services, but for the most part Oracle is the prevalent database software in use at the City. An initial review of the Oracle environment indicated that databases for the more complex or larger systems, such as the Tax and Water billing system, the SAP financial information and human resources systems, or those that cross department boundaries are the responsibility of the Information & Technology Division of the Corporate Services Department. Departmental database administrators are responsible for the management of smaller databases, which are unique to individual departments.

Our review focused on the security practices in effect for the more significant and critical Oracle databases controlled by the Information & Technology Division within the Corporate Services Department.

The objectives of our review were to assess the extent to which:

- the Information & Technology Division of the Corporate Services Department has systems and procedures in place to minimize database security related risks that would impede the attainment of business objectives;
- the security procedures are in accordance with best practices; and
- these systems and procedures are carried out in a cost-effective manner with due regard for economy and efficiency.

A summary of the major issues identified during our review is included in the following Summary of Significant Audit Observations. Details supporting these observations, along with our recommendations, are provided in the body of the report.

Summary of Significant Audit Observations

1. Issues identified and recommendations contained in this report likely have relevance not only to the Information & Technology Division but also to other City Departments as well as the Agencies, Boards and Commissions.

2. There is no central City resource responsible for ensuring that effective Oracle database security policies are developed, circulated, promoted and monitored throughout the City. Security concerns are currently the responsibility of various database administrators, either within the Information & Technology Division or within departments.
3. There is a need to prepare a City-wide protocol and process for the development, approval and communication of all new or revised information technology security policies and procedures.
4. There is no central resource responsible for the administration of security alerts. Business cases relating to the costs and benefits of responding to certain security alerts are not completed.
5. Oracle software contains a large number of default administrative user accounts, each with a default password. Failure to change these well-known default passwords increases the potential for unauthorized access to the system. Default accounts and passwords were not always changed.
6. Oracle software includes many security features one of which is the auditing feature. One of the purposes of the auditing feature is to monitor access to the database. The activation of the auditing feature, however, slows down employee access to the system and generally is one of the reasons why in certain organizations the feature has been deactivated. At the City the auditing feature has been activated for certain databases but not for others. The decision to not fully activate the auditing feature was conducted without any formal analysis in terms of the access risks which the City may be subject to.
7. The backup and recovery procedures for the Oracle databases are not formalized, documented and integrated into the overall Corporate Database Group's business continuity plan. The plan is not tested on a regular basis to ensure the ability to provide database processing in the event of a disaster.
8. The Information & Technology Division is responsible for managing the City's Oracle licenses, but does not have any jurisdiction over departmental Oracle users. For example, the Division cannot determine the number of registered users to ensure the City has not exceeded its authorized licence usage. Processes should be in place to allow the Division the necessary authority to fulfil this responsibility.

Detailed comments in relation to the Summary of Significant Audit Observations are contained in the following paragraphs.

Comments:

Recommendations contained in this report may have relevance to all databases throughout the City as well as those managed by the Information & Technology Division. In addition, the recommendations may also have relevance to databases at the City's Agencies, Boards and Commissions. Consequently, it is suggested that the report be forwarded to each one of these entities for their review, analysis and consideration.

In addition while this report has identified certain weaknesses in the City's security procedures relating to the Oracle database environment it has not addressed security weaknesses which may exist in other general applications throughout the City.

The Auditor General's office at the present time will not be conducting further security reviews in 2004 and as a result it is suggested that the Information & Technology Division conduct its own internal evaluation of all security practices. In this context, specific security related audit programs are available from various sources. One of the best sources in this regard is published by the United States General Accounting Office entitled "Federal Information System Controls Audit Manual". While this manual is specifically applicable to auditors there is no reason why staff should not be able to conduct their own self audit in order to satisfy themselves that security practices are appropriate and effective. A further publication entitled "Oracle Security Step-by-Step: A Survival Guide for Oracle Security" is also available.

As part of our 2005 work plan we anticipate reviewing the results of the self assessment audit conducted by the Information & Technology Division and conducting specific audit work on the self assessments in order to ensure that they are accurate and also to ensure that known deficiencies identified as a result of this review have been addressed.

Recommendations:

1. City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and report to the July 2004 meeting of Audit Committee on the results of their reviews including any action taken.
2. The Commissioner of Corporate Services, direct that a self-assessment security audit be conducted on all major computer applications directly supported by the Information & Technology Division. In conducting this audit, consideration be given to the audit steps contained in various publications including the publication of the United States General Accounting Office entitled "Federal Information System Controls Audit Manual" and the publication entitled "Oracle Security Step-by-Step: A Survival Guide for Oracle Security". Copies of all such self-assessment audit reports be forwarded to the Auditor General's Office for review, evaluation and subsequent audit.

General Organization Control

In large organizations such as the City, best practices require that a dedicated security officer should be responsible and accountable for data-security policies throughout the City.

Our review identified the following:

- there is no one area or employee responsible for ensuring that effective Oracle database security policies are crafted, circulated, promoted and monitored throughout the City;
- there are no approved database security standards and policies to guide individual database administrators responsible for the City's critical systems; and

- database administrators are required to address security issues along with all the other administrative tasks for which they are accountable.

Our comments in connection with this particular issue are similar to those presented in our “Information Security Framework” report dated January 26, 2001. That report recommended a corporate-wide Information Security Program, which would be centrally administered and supported with the appropriate level of resources. While the City has taken initial steps in implementing certain of the recommendations from this particular report, other recommendations and in particular, the creation of a data security function have not been fully addressed.

The creation of a data security function with responsibility for establishing a security plan for all databases throughout the City would provide assurance that the security policies and procedures are appropriate, consistent and adequate.

Responsibilities of a centralized security function should include but not be limited to the following:

- coordinating the development of and distributing security policies and procedures;
- routinely monitoring compliance with these policies;
- promoting security awareness among system users; and
- providing reports to senior managers on policy and control.

Recommendations:

3. The Commissioner of Corporate Services, provide a written response to the Audit Report dated January 26, 2001, entitled “Information Security Framework” and forward such report to the July 13, 2004 meeting of the Audit Committee. The report from the Commissioner should include an update on the action taken on the recommendations included in the report dated January 26, 2001.
4. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report to the City’s Administration Committee on the benefits and costs of establishing a centralized database security function with authority to administer and monitor database security practices for all databases throughout the City.

Oracle Database Security Standards and Procedures

Best business practice requires security policies to be formulated and communicated. Security policies state what an employee can and cannot do. The existence of such policies is even more important in an organization such as the City where there is decentralized administration of certain databases. Well thought out and articulated security policies and procedures provide greater assurance that database security practices are consistently applied throughout the organization and provides a standard to guide staff in their activities.

Currently in the City:

- the “Oracle Database Standards and Procedures” document, authored by the Information & Technology Division in the first half of 2002 remains in draft form;
- there are no City-wide security standards for administering and using database assets in the City;
- the section on security in the “Oracle Database Standards and Procedures” is inadequate in content; and
- there is no predefined process for approval of new or revised departmental and/or corporate policies and procedures.

Recommendation:

5. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, prepare a City-wide protocol and process for the development, approval, implementation and communication of all new or revised information technology policies and procedures. In addition, the Commissioner of Corporate Services, finalize the “Oracle Database Standards and Procedures” document ensuring it adequately addresses Oracle security.

Maintaining the Oracle Software

The trend within the software industry is to deliver a product to the market as quickly as possible. In such circumstances, the software may have certain security weaknesses which were not identified at the time of delivery.

As the software vendors become aware of and identify security weaknesses, they issue security alerts and send software revisions called “patches” to their customers to allow them to remedy the identified weaknesses. If a customer has software containing one of these weaknesses, it is important to remedy or patch the weakness as soon as possible prior to the weakness being taken advantage of.

Our review of the City’s practice in handling patches and security alerts included an examination of the Web site of the Oracle Corporation. Our research indicated that there were approximately 400 patches or security alerts relating to the family of Oracle database software currently in use at the City. Depending on how the Oracle software has been installed at the City will determine whether or not an individual patch needs to be applied. Nevertheless installing a patch requires that the system be shut down to day to day users. Although the patch can be applied in off peak hours, it still requires staff resources as every time a patch is applied, there are significant procedures involved to ensure it has been done correctly and the software continues to operate as intended.

The responsibility of all database administrators is to make themselves aware of security patches as soon as possible and then to assess whether or not the particular patch needs to be applied to the Oracle software supporting their particular database. Depending on the application, not all patches are required.

City staff monitors security alerts from the Oracle Corporation. Although patches to the software are installed after an internal analysis by the Corporate Database Group within the Information & Technology Division, our review identified that:

- the City does not formally assess the exposure and potential impact an identified weakness could have on business operations or data against the effort and cost required to apply the patch; and
- responsibility for disseminating security alerts and patches to database administrators throughout the City has not been formalized.

The current practice for handling patches throughout the Corporation is informal and inconsistent and increases the possibility that the installation of patches may not be appropriately administered.

Recommendation:

6. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the current practices in connection with the installation of software patches to Oracle and other software applications. Such a review ensure that:
 - a. an analysis is done to ensure that the benefits of installing specific software patches outweigh the risk and costs inherent in not applying the software patches;
 - b. a process be implemented in order to ensure that information in regard to software patches is disseminated throughout the City; and
 - c. patches, where required, have been appropriately and consistently installed.

Oracle Security Features

Oracle software includes many security features, one of which can be used to monitor who accesses the database, when and from where. It also provides an audit trail for modifications to the database. The downside of activating this feature is the increased demand for system resources and a potential negative impact on overall system performance. As a result of the potential impact on system performance and without any in depth analysis, the “audit trail” feature is not often activated.

The decision to not use this feature should be a business decision taken after considering the benefit of auditing certain transactions against the potential for negative impacts on system performance or the cost or need for additional resources required to effectively use this feature.

Activation of the auditing feature improves the City’s ability to determine if someone is attempting to gain unauthorized access to the database. The feature can also provide critical information when it is determined that someone is in the process of attempting to gain unauthorized access. Further, the use of the auditing feature will enhance the opportunity to investigate and repair on a timely basis, improper changes to original data. One subset of the auditing feature, auditing of failed logins for all accounts, should always be enabled as an aid to identify inappropriate access attempts.

The auditing feature is not used extensively in the City and there is no documentation to support that this decision was taken as a result of investigating what actions should be “audited” and the impact such action would have on overall performance or cost of operating the system.

Recommendation:

7. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the extent to which Oracle’s standard auditing features should be activated and this process be implemented corporate wide. Any decisions in relation to the activation or otherwise should be documented and approved by supervisory staff. As a minimum, we recommend the logging and timely review of unsuccessful access attempts.

Default Accounts and Passwords

Similar to most software, Oracle software is provided with a large number of default user accounts, each with a default password that can be installed as part of an Oracle installation. These default accounts are necessary to allow the database administrator to set-up and maintain the software. As such, these user accounts give very broad access and powers to the individuals assigned to them.

The confidentiality and integrity of data can be compromised by the misuse of default accounts that are automatically installed with well-known default passwords. These accounts provide the easiest way for someone to enter the database. Users should be restricted from accessing databases through vendor provided default usernames and associated passwords.

As a part of our review, we analyzed the password files for the default accounts in six different Oracle systems. Our review identified eight instances where the default password supplied with the software had never been changed. In response to our findings, we immediately discussed this matter with staff from the Information & Technology Division. We have been advised that each database administrator reporting to the Information & Technology Division has been directed to review passwords for all Oracle default accounts in order to ensure that all such passwords are changed immediately. To the best of our knowledge, this direction has not been provided to departmental administrators.

Oracle Listener Program Security

The Oracle Listener software is a part of the Oracle software that manages connections to the Oracle databases by individuals not connected directly to the network. The Oracle Listener, for example, is required when a staff member is required to access the network from a remote location. A weakness exists in some versions of the Oracle Listener program when a unique password is not assigned to this program. Where this weakness is present it allows an unauthorized person to log onto the Listener and perform various tasks, including gaining access to the data.

This is a significant security weakness and is currently present in the SAP financial information system and the IBMS building permits system.

Recommendation:

8. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, direct database administrators throughout the City to review all passwords for default accounts provided by the Oracle Corporation in order to ensure that all such default passwords have been changed. Passwords be changed, where appropriate.

Continuity of Database Operations

Computers, and consequently databases, are susceptible to a wide range of external events such as theft or fire. In addition, the loss of power to a computer could render it inoperable until power is restored. The loss of critical data or computing facilities could result in significant financial losses to the City. Best practice and prudent management requires that there be a plan on how to recover from these events regardless of how unlikely they may seem. Such a plan, often called a business continuity plan, provides the framework for a controlled response to emergency situations.

A comprehensive business continuity plan normally involves various levels of management and crosses many organizational units. The plan would detail a step by step approach to ensure access to critical data is restored quickly enough to minimize the operational and financial impacts of any event affecting the availability of the data. These business continuity plans are developed on various levels such as for individual software, physical locations and databases.

The "Oracle Database Standards and Procedures" document alluded to earlier in this report contains sections on Backup, Recovery and Disaster Recovery applicable to database components directly under the control of the Corporate Database Group in the Information & Technology Division. However, the content of this document is descriptive and general in nature. It is not written for specific databases with details such as; file names, file paths, etc., for each application. In addition, the backup and recovery procedures are not integrated into a business continuity plan, increasing the risk to a successful recovery of data and operations.

Recommendation:

9. The Commissioner of Corporate Services update, document and test the database business continuity plan for the databases administered by the Information & Technology Division and such documentation be centrally maintained.

Managing Oracle Databases Licenses

The Information & Technology Division is responsible for the management of Oracle licenses. These are "name user" licenses which signify that once an employee is granted such a licence, they are entitled to access any Oracle database within the City.

The City also has licences referred to as "Power Units" to accommodate access to Oracle databases through various Web based systems. An example of such a system is the Food Premises Inspection and Disclosure system, which allows the general public to obtain the "Dine Safe" status of various establishments.

Although the Information & Technology Division has assumed responsibility for managing these Oracle licenses, the Division does not have the authority necessary to fulfil this responsibility. While the Division is accountable for managing the Oracle licenses for the entire City, it has no jurisdiction over departmental Oracle users. For example, the Unit has neither the authority to query a departmental database to ascertain the number of licenses in use nor the right to verify whether an existing user or new user added to a department-controlled database is valid and not duplicated. The absence of the ability to verify such information makes it very difficult for the Division to effectively manage the Oracle licenses.

Despite the limitation described above, in the first quarter of 2003, staff within the Division began several initiatives and, in conjunction with database administrators from various departments, identified 4,589 redundant licenses. These redundant licenses arose where a staff member accessed two different Oracle databases. This was counted as two users when, in fact, there is only one user and therefore only one license is required.

The City cannot effectively and efficiently manage its Oracle licenses in a cost-effective manner while the Division's authority is not commensurate with its responsibilities. Generally, for departmental Oracle databases, the Division has to rely on the department's database representative to inform them of the number of Oracle licenses in use rather than being able to query the system directly. This increases the risk that the City could be in violation of software licensing agreements or, alternatively, that the City could fail to realize cost savings by identifying opportunities to reduce the number of licenses.

Recommendation:

10. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, take the necessary steps to centralize, within the City's Information & Technology Division, the custody, recording and administration of all Oracle database software licenses for the City.

Reporting Back to the Audit Committee

In order to ensure that the issues identified in this report are addressed expeditiously, it is suggested that there be a reporting process back to the Audit Committee, on a timetable regarding the implementation of the recommendations contained in this report.

Recommendation:

11. The Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.

Conclusions:

Data contained within the City's computer systems is one of its most important assets. The protection of this data is of paramount importance. The design and implementation of effective, efficient security policies and procedures is necessary to minimize the City's exposure to

intentional or accidental access to such data. Should security be inadequate to prevent access to the City's data, it could be rendered unreliable or unavailable, preventing departments from conducting business and potentially leading to an inability to deliver essential services, a loss of revenue and inadequate control over its assets.

In this report, we have identified and made recommendations in connection with the following:

- the need to ensure that the recommendations in this report are considered by all Departments, Agencies, Boards and Commissions;
- the need to implement a self assessment security evaluation of all applications throughout the City;
- the need to develop a central resource to assume responsibility for City-wide corporate security issues;
- the need to develop consistent policies and procedures relating to the application of security patches throughout the City of Toronto;
- the need to ensure that all default security passwords issued by the Oracle Corporation are changed immediately;
- the need to evaluate the costs and benefits of implementing certain audit features of the Oracle software; and
- the need to centrally manage all Oracle software licenses.

Addressing the recommendations outlined in this report will strengthen overall data security in the City and protect one of its most important assets.

Contact:

Jerry Shaubel
Director, Auditor General's Office
Tel: (416) 392-8462, Fax: (416) 392-3754
e-mail: JShaubel@toronto.ca

Ben Smid
Senior Audit Manager, Auditor General's Office
Tel: (416) 392-8478, Fax: (416) 392-3754
e-mail: BSmid@toronto.ca

The Audit Committee also submits the joint report (February 10, 2004) from the Chief Administrative Officer and Commissioner of Corporate Services:

Purpose:

To provide a management response to the recommendations contained in the Auditor General's Report titled "Oracle Database Review – Security Controls and Other Issues" submitted to the Audit Committee for its meeting on February 24, 2004.

Financial Implications and Impact Statement:

There are no immediate financial implications as a result of this report.

Recommendation:

It is recommended that this report be received for information.

Background:

At its scheduled meeting of February 24, 2004, the Audit Committee will be considering a report from the Auditor General on the results of his review of security controls relating to the City's Oracle databases managed by the Information & Technology Division of the Corporate Services Department.

The Chief Administrative Officer and the Commissioner of Corporate Services submit this report to provide a management response to the recommendations contained in the Auditor General's report

The Chief Administrative Officer and the Commissioner of Corporate Services are in agreement with the Auditor General's recommendations. It should be noted that, while the original review was focused only on the Oracle databases managed by the Information & Technology Division in Corporate Services Department, the recommendations are enterprise in nature and affect all City departments and potentially its Agencies, Boards and Commissions. The Information & Technology Division has already taken steps within its operations to implement some of the recommendations.

In addition, we suggest that the recommendations not be limited to Oracles database systems but all other database products as well, such as Microsoft SQL and IBM DB2. Appendix A to this report provides the management response to the Auditor General's recommendations.

Conclusions:

The recommendations contained in the Auditor General's report are enterprise in nature and affect all City departments and potentially its Agencies, Boards and Commissions. The Chief Administrative Officer and the Commissioner of Corporate Services are in agreement with the Auditor General's recommendations and have provided further comments as a management response. The Information & Technology Division has already taken steps within its operations to implement some of the recommendations.

Contacts:

Ana Bassios
Acting Executive Director
Information & Technology Division
Corporate Services Department

Tel: (416) 392-8421
E-Mail: abassios@toronto.ca

Stephen Wong
Director
Information & Application Services
Information & Technology Division
Corporate Services Department
Tel: (416) 397-9175
E-Mail: swong@toronto.ca

Appendix A

Management Response to the Auditor General’s Report on Oracle Database Review
 - Security Controls and Other Issues

| Recommendation | Management Response |
|---|---|
| <p>(1) City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and report to the July 2004 meeting of Audit Committee on the results of their reviews including any action taken</p> | <p>Agreed.</p> |
| <p>(2) the Commissioner of Corporate Services, direct that a self-assessment security audit be conducted on all major computer applications directly supported by the Information & Technology Division. In conducting this audit, consideration be given to the audit steps contained in various publications including the publication of the United States General Accounting Office entitled “Federal Information System Controls Audit Manual” and the publication entitled “Oracle Security Step-by-Step: A Survival Guide for Oracle Security.” Copies of all such self-assessment audit reports be forwarded to the Auditor General’s Office for review, evaluation and subsequent audit;</p> | <p>The recommendation extends beyond the original focus on the security of the underlying Oracle databases in major applications supported by the Information & Technology Division to include the overall security of the corresponding major applications themselves as well. Management agrees with this extended approach to better assess the overall security for the City’s major computer systems, and suggests that the same security assessment be conducted on major departmental applications as a future next step.</p> <p>Industry best practices will be utilized in conducting the self-assessment security audits including those contained in the suggested publications. Conducting self-assessment security audits on all major computer applications directly supported by the Information & Technology Division would require significant efforts and a level of auditing expertise and discipline that is not generally required in I&T’s day-to-day operations. In this respect, we will seek the Auditor General’s advice while conducting the self-assessment security audits. Staff will establish timelines for this component in the workplan report required by Recommendation (11) of this report.</p> |
| <p>(3) the Commissioner of Corporate Services, provide a written response to the Audit Report dated January 26, 2001, entitled “Information Security Framework” and forward such report to the July 13, 2004 meeting of the Audit</p> | <p>Since the “Information Security Framework” Audit Report, the Information & Technology Division has recruited a Director, Information & Technology Planning who has responsibility for overall security policies and procedures. A full-</p> |

| Recommendation | Management Response |
|--|--|
| <p>Committee. The report from the Commissioner should include an update on the action taken on the recommendations included in the report dated January 26, 2001;</p> | <p>time Security Policy Analyst position has also been filled to review security from an enterprise perspective. This includes the development of a security framework, associated policies, and periodic audits and reviews. As part of the Digital Academy speaker series to raise information technology awareness within the City, information sessions were held with senior staff and councillors to discuss the need for security within organizations and the associated information systems. A comprehensive response to the “Information Security Framework” report will be made to the Audit Committee to explain in detail all steps taken and progress made.</p> |
| <p>(4) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report to the City’s Administration Committee on the benefits and costs of establishing a centralized database security function with authority to administer and monitor database security practices for all databases throughout the City;</p> | <p>Management agrees with this recommendation. This task requires extensive consultation and operational review and staff will provide a plan for addressing this recommendation in the workplan to come to Audit Committee in July 2004, and will report out further to Administration Committee thereafter.</p> |
| <p>(5) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, prepare a City-wide protocol and process for the development, approval, implementation and communication of all new or revised information technology policies and procedures. In addition, the Commissioner of Corporate Services, finalize the “Oracle Database Standards and Procedures” document ensuring it adequately addresses Oracle security;</p> | <p>Management agrees with this recommendation.</p> <p>The Information & Technology Division has a working protocol and process for the development, approval, implementation and communication of information technology policies and procedures. This working protocol and process will be reviewed and updated for formal adoption as a City-wide protocol and process. In consultation with the information technology standards working group with representatives from all departments, the document titled “Oracle Database Standards and Procedures” will be updated and finalized for management approval and implementation. Implementation will be completed by July 2004.</p> |
| <p>(6) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the current practices in connection with the installation of software patches to Oracle and other software applications. Such a review ensure that:</p> | <p>Management agrees with this recommendation. Effective patch management should be for all software in the City and not just the Oracle database software.</p> <p>Decisions to install software patches rely on the understanding of the business and technical needs and an assessment of the associated risks</p> |

| Recommendation | Management Response |
|---|---|
| <p>(a) an analysis is done to ensure that the benefits of installing specific software patches outweigh the risk and costs inherent in not applying the software patches;</p> <p>(b) a process be implemented in order to ensure that information in regard to software patches is disseminated throughout the City; and</p> <p>(c) patches, where required, have been appropriately and consistently installed.</p> | <p>in applying the patches and the impacts they will have on the application environment. There are existing documented technical operational procedures, including problem and change management processes, within the Information & Technology Division that are used for applying software patches.</p> <p>This will impact some departmental IT areas where formal processes or accountability might not exist today. The Corporate Services Information & Technology Division will take the lead to identify, co-ordinate and manage an enterprise-wide software patch management process. The use of software to assist in managing such a process will be investigated.</p> |
| <p>(7) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, review the extent to which Oracle's standard auditing features should be activated and this process be implemented corporate wide. Any decisions in relation to the activation or otherwise should be documented and approved by supervisory staff. As a minimum, we recommend the logging and timely review of unsuccessful access attempts;</p> | <p>Currently, Corporate Services I&T already have this feature enabled for a number of critical systems. Implementing Oracle's standard auditing features on databases will have a significant negative impact on the performance of the application hardware and potentially may result in a service level degradation of the corresponding applications.</p> <p>In reviewing the implementation of enablement of the Oracle standard auditing features, consideration will be given to the criticality of the subject applications, impact on the application users, and any hardware upgrades which might be required to maintain system performance within acceptable limits. A standard management process where the logging of unsuccessful Oracle database access attempts are flagged, captured, and reviewed will be implemented as recommended by September 2004.</p> |
| <p>(8) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, direct database administrators throughout the City to review all passwords for default accounts provided by the Oracle Corporation in order to ensure that all such default passwords have been changed. Passwords be changed where appropriate;</p> | <p>Management agrees with this recommendation. A communication will be sent to all database administrators before March 31, 2004.</p> |

| Recommendation | Management Response |
|--|--|
| <p>(9) the Commissioner of Corporate Services update, document and test the database business continuity plan for the databases administered by the Information & Technology Division and such documentation be centrally maintained;</p> | <p>The City has signed a contract with Sunguard Recovery Services to assist Corporate Services I&T and its business clients in the review and development of a business continuity plan. This exercise not only will review the recovery processes from a business perspective should technology fail, but also the associated technology capabilities to ensure that recoveries can be achieved within a reasonable period of time. The findings and recommendations of this business continuity plan review will be the subject of a future report, planned for Administration Committee in October 2004.</p> <p>Corporate Services I&T have in place documented technical procedures for database and application recoveries in the event of technical system failures.</p> |
| <p>(10) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, take the necessary steps to centralize, within the City's Information & Technology Division, the custody, recording and administration of all Oracle database software licenses for the City; and</p> | <p>Management agrees with this recommendation. Currently, for the systems managed by Corporate Services I&T, agent technology is used to assist in gathering information for report on Oracle database software license usage.</p> |
| <p>(11) the Commissioner of Corporate Services, in consultation with the Chief Administrative Officer, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.</p> | <p>Management agrees with this recommendation.</p> |