TORONTO PUBLIC LIBRARY

Oracle Database Review – Security Controls and Other Issues
Toronto Public Library Management Response

	Recommendation	City Management Response	TPL Management Response	Status and Timeline for implementation
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.	Agreed.	Agreed.	TPL response to be presented to the TPL Board at its June 14th meeting for information prior to forwarding TPL's response to the Audit Committee for its meeting on July 13th.
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.	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. 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	TPL agrees with extending the focus to include major applications. The Library does not have expertise in security audits and proposes to seek external assistance to perform a self-assessment security audit. External assistance would allow us to include a knowledge transfer component and develop internal expertise.	Planning for the security audit will take place in 2004, with actual work to be accomplished by December 2005.

	Recommendation	City Management Response	TPL Management Response	Status and Timeline for implementation
		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.		
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.	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-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.	No action required from the Library.	
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.	Management agrees with this recommendation. This task required 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.	Administration and monitoring of the Oracle databases is centralized at TPL and assigned to the Senior Database Administrator.	No further action.

	Recommendation	City Management Response	TPL Management Response	Status and Timeline for implementation
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.	Management agrees with this recommendation. 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.	The Library has a defined process for the development, approval and communication of policies and procedures, which applies to IT policies and procedures. The Library will review the City's "Oracle Database Standards and Procedures" once approved and determine what aspects apply to the Library and draft a Library policy.	Review to be undertaken in 2004, with development of Library policy and implementation in 2005.
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 ensures 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) 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	Management agrees with this recommendation. Effective patch management should be for all software in the City and not just the Oracle database software. Decisions to install software patches rely on the understanding of the business and technical needs and an assessment of the associated risks 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. 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	TPL agrees with this recommendation. Decisions to install software patches rely on the understanding of the business and technical needs and an assessment of the associated risks in applying the patches and the impacts they will have on the application environment. There are existing documented technical operational procedures within the Library's Information Technology Department that are used for applying server operating system software patches. Software patches for Oracle and other databases are reviewed before applying. Procedures need to be formally documented. Administration of all Library databases is centralized and reduces the risks of inconsistent application.	Formal documentation for Oracle database software patch management will be incorporated into the software patch management process review planned for 2005.

	Recommendation	City Management Response	TPL Management Response	Status and Timeline for implementation
	installed.	software patch management process. The use of software to assist in managing such a process will be investigated.		
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.	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. 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.	Library Management agrees with the minimum recommendation for the logging and timely review of unsuccessful access attempts. The other auditing features will need further investigation to determine the negative impact they will have on performance and the costs associated with system upgrades to maintain performance.	Logging and review of unsuccessful access attempts for Oracle databases will be implemented in June 2004. Investigation of other auditing features will be conducted in 2005.
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.	Management agrees with this recommendation. A communication will be sent to all database administrators before March 31, 2004.	The Library has verified that it does not have any default accounts. This is in keeping with IT standard practice for all systems. The Library does not use default accounts and passwords.	In compliance with audit recommendations.

	Recommendation	City Management Response	TPL Management Response	Status and Timeline for implementation
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.	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. Corporate Services I&T have in place documented technical procedures for database and application recoveries in the event of technical system failures.	The Library is developing a Disaster Recovery Plan that will incorporate a business continuity plan. The Library already has automated backups in place for all databases. The Library has set up and tested database recovery scripts. The Oracle database backups are stored off-site.	The Disaster Recovery Plan will be developed in 2005.
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.	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.	The Library has centralized the custody, recording and administration of all Oracle database software licenses within the Library's IT department.	In compliance with the audit recommendations.
11	The Commissioner of Corporate Services, in consultation with the CAO, report back to the Audit Committee scheduled for July 13, 2004, on a workplan in regard to the implementation of the recommendations contained in the "Oracle Database Review – Security Controls and Other Issues" report. Such report to include specific timelines for implementation.	Management agrees with this recommendation.	TPL agrees with this recommendation.	