APPENDIX 2

TORONTO

Memorandum

Information & Technology
Dave Wallace, Chief Information Officer

Metro Hall
55 John Street
15th Floor
Toronto, Ontario M5V 3C6

Tel: 416 392-8421
Fax: 416 696-4244
dwwallace@toronto.ca
www.toronto.ca

April 3, 2008

To: **Audit Committee**

From: **Dave Wallace, Chief Information Officer**

Subject: **Management Response to the Auditor General's Review of Disaster Recovery Planning for City Computer Facilities**

The Information & Technology Division's Management Response to the Auditor General's report is attached. I would like to commend the Auditor General for this report. We believe it is insightful and accurately depicts the state of IT Disaster Recovery at the City. We are committed to ensuring that we are able to maintain critical information technology systems and critical services for the people of Toronto in the event of a disaster. This response indicates our agreement with the recommendations and provides an action plan to address them.

I would also like to thank the Auditor General for recognizing the successful effort of the Information & Technology Division toward ensuring the high availability of the City's information systems that we manage from our primary data centre. We have invested in creating a resilient environment for our technology infrastructure at this data centre and into the facility itself. As a result, the probability of a significant failure within our data centre is extremely low. A partial list of these measures includes:

Systems and Technology High Availability Measures

- Duplicate (clustering) server hardware and storage disks with software failover and load balancing to provide redundancy and ensure business systems availability if a component fails
- Large enterprise servers have error correcting memory and memory reallocation and multiple redundancy components in large enterprise servers
- Server virtualization, which permits provisioning of an application or database server in under 1 hour (previously this took several hours or more than a day)
- Dual electrical feeds from all servers into separate building electrical panels
- Monitoring software which provides threshold-based alerts to technical support staff
- Significant investments in security appliances and software and external intrusion detection services to prevent malicious software attacks
- Significant on-going investment and commitment to best practice processes
- 7x24x365 staffing of the data centre to provide human monitoring and intervention
- Technical support staff on call, with remote access capability to troubleshoot and restore
- Virus protection on all desktops, servers, and virus appliances scanning internet traffic, and email scanning appliances for incoming and outgoing email

Facility High Availability Measures

- Building structural reinforcement, to resist the impact of earthquakes
- Dual electrical supply feeds into the building from separate electrical sub-stations
- Dual water supply into the building, to ensure water cooling is always available
- Dual UPS banks to provide continuous short-term electrical supply
- Dual diesel generators, for continuous long-term power in the event of major power failure
- Specialized data centre fire suppression systems

While these investments are on-going as new technical challenges emerge or opportunities for improvements are identified – the systems managed from our primary data centre have achieved a very high availability, exceeding 99.9 %. For the Program Areas, this level of availability ensures the productivity of their staff as they become more reliant on information technology to perform their jobs most effectively. In addition, it builds confidence in the reliability of online services to the public, who will increasingly be using this channel to receive services from the City.

Next Step: Eliminating the Data Centre as Single Point of Failure

While we have successfully achieved high availability within the data centre through eliminating single points of failure, and the probability of extended failure is very low, the Auditor General has correctly noted that the data centre facility itself can be a single point of failure. Major disasters that could take out part or all of the data centre's ability to provide service are unlikely; however they can occur and we must eliminate this final single point of failure as it would have serious impacts for the City.

The Information & Technology Division has recently started a disaster recovery planning program. We have commenced the development of a long-term data centre strategy which will incorporate disaster recovery. We have also invested in a secondary data centre facility which became operational in September, 2007. This facility has considerable infrastructure now in place to permit us to start our program of being able to recover systems in the event of a disaster at our primary data centre. Achievements to date include:

- Alternate data centre has been constructed and is operational
- Core infrastructure is in place and we have already reduced the time to recover from disaster
    - Up to 150 servers can now be accommodated within the alternative facility
    - Networking and storage is in place to accommodate DR servers
    - Tape library is installed so that we can recover from tape to application servers
    - Base infrastructure servers to facilitate authentication onto the City Network are deployed at this site
    - Network connectivity to major City sites is in place
    - Currently able to connect to the EDS Mainframe via backup network link

- Office of Emergency Management are aware of the IT-DR program and we are working together
- Disaster Recovery Plan document has been prepared which provides a range of procedures and programming scripts to initiate in the event of disaster
- Vital records are now being stored at both the primary and secondary site to ensure their availability (e.g. contact lists, installation media, source code, patches, licence information, product keys, access codes and passwords)

- Detailed planning, architecture, design, implementation, recovery system documentation and testing for SAP and GroupWise Email are now underway, for completion before end of 2008 (this will reduce the recovery time for these key systems to 2-3 days in the event of a disaster).

Disaster Recovery is a Cost of Doing Business

The Auditor General's report essentially notes that IT Disaster Recovery programs are a necessary cost of doing business, particularly so for the City which provides essential citizen services. Substantial Disaster Recovery programs require adequate capital and operating investments. They involve building and managing a secondary data centre. Duplicate hardware and software and network infrastructure must be acquired and maintained to permit rapid recovery. As our Management Response indicates, we will be detailing a program for our capital and operating budgets, as well as completing the IT Governance required to adequately support a co-ordinated IT Disaster Recovery program for all City divisions. We will also work closely with the ABC's to ensure collaboration on these initiatives.

I would like to again thank the Auditor General's office for their report, which I believe has raised the profile of this important subject. We are committed to completing the action plan to address their recommendations.

Dave Wallace
Chief Information Officer

APPENDIX 2

Management's Response to the Auditor General's Review of Disaster Recovery Planning for City Computer Facilities

Rec No	Recommendation	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
1.	**The City Manager develop a formal disaster recovery planning and preparedness protocol with the Agencies, Boards and Commissions. The protocol should ensure coordination, collaboration and communication related to computer facility disaster recovery planning and preparedness**	**X**		We agree that there are opportunities for the City's I&T Division and the ABC's to collaborate. Discussions have already taken place to promote consistency in architecture and standards, to achieve economies of scale and to share best practices, in such areas as: - Data centre strategy (primary and alternative DR sites) - Data communications network - Sharing of geospatial technical environment.	• A formal IT-DR planning and preparedness protocol will be developed. • Timing: by October, 2008
2.	**The City Manager implement a disaster recovery and business continuity program that includes divisional roles and responsibilities, resource and training requirements, and simulation and plan maintenance schedules.**	**X**		As noted in the report, IT- DR is a subset of overall Business Continuity Planning (BCP). Often IT-DR planning is a catalyst for considering full BCP and the I&T Division has already contacted the Office of Emergency Management to discuss the role of IT-DR within the City's emergency planning process. I&T Division can assist with BCP by using expertise in overall Risk Management and DR planning to develop an integrated approach to BCP/IT-DR. Overall responsibility for BCP ultimately lies with each division.	• Working with the City Manager's Office, the Office of Emergency Management and divisions, Information & Technology Division will facilitate the establishment of a BCP and IT-DR program and framework. • Timing: May, 2009 to have the planning framework in place along with BCP/IT-DR governance defined and program planning commenced.

APPENDIX 2

Management's Response to the Auditor General's Review of Disaster Recovery Planning for City Computer Facilities

Rec No	Recommendation	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
3.	**The Chief Information Officer to report to the Business Advisory Panel on a periodic basis. Such reporting to include updates on disaster recovery planning and preparedness for information technology systems**	**X**		The IT Governance initiative has established the Business Advisory Panel (BAP) along with an Enterprise Architecture Review Panel to direct overall I&T strategy and investment priorities. IT-DR will be an important facet of the I&T strategy and will be a specific agenda item at least once or more per year. The initial report will provide a working paper to identify the preliminary IT-DR strategy and the associated capital and operating investment plan. It will also define the governance model which will permit the BAP to determine investment levels and sequence priorities to have City information systems complete the IT-DR planning and implementation process.	• The CIO will ensure an annual or more frequent report to the BAP in the status of IT disaster recovery planning and preparedness. • Timing: Initial report, including preliminary strategy, investment plan and governance model will be provided to BAP by July, 2008.
4.	**The Chief Information Officer take action to ensure management responsible for maintaining City computer systems receive timely direction, guidance and training on preparing consistent City-wide disaster recovery plans.**	**X**		The I&T Division has already begun preparation of an IT-DR planning framework/process, which is going through an initial cycle with: - SAP - GroupWise Email	• A full training program for those responsible for IT-DR planning and testing will be developed and offered to: - Applicable management and practitioners within the I&T

Management's Response to the Auditor General's Review of Disaster Recovery Planning for City Computer Facilities

Rec No	Recommendation	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
				This will ensure these systems can be quickly restored (within 2-3 days) in the event of a primary data centre disaster. Once completed, this process can be repeated for other systems and a training program can be initiated.	Division - Directors and IT Managers within divisions responsible for IT systems - ABC IT Managers • Timing: May, 2009
5.	**The Chief Information Officer review the backup and storage procedures of City information technology units for:** **(a) compliance with acceptable standards and practices for data backup and storage requirements; and** **(b) provide divisions with the opportunity to participate in existing data storage arrangements within the City or with an outside service provider.**	**X** **X**		Information & Technology Division has a solid backup and storage process in place. We currently use an external service provider to store our backup media. All documentation is maintained at both our primary and alternative data centre facility. It should be noted that at the conclusion of the IT Governance and Reorganization currently underway, most of the responsibility for IT infrastructure will be centralized within the Information & Technology Division.	• Information & Technology Division will publish best practices for data backup and storage and ensure divisional IT compliance. • Timing: November, 2008 • Develop a plan to have divisions participate in I&T Division's date storage and backup services, including a review of logical migration of infrastructure into centralized facilities. • Timing: November, 2008
6.	**The City Manager, in consultation with the Chief Information Officer, direct divisions to test information technology disaster recovery plans on a regular basis.**	**X**		Information & Technology Division has previously initiated a testing process with the outsourced EDS mainframe contract.	• A process will be established to ensure all stakeholders participate in a regular testing cycle for the IT-DR plans, once

Management's Response to the Auditor General's Review of Disaster Recovery Planning for City Computer Facilities

Rec No	Recommendation	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
				Testing of the initial infrastructure at the alternative data centre has begun and testing will be part of the IT-DR methodology being established.	established. • Timing: March, 2009
7.	**The Chief Information Officer develop disaster recovery testing guidelines and provide training necessary to ensure cross-divisional consistency**	**X**			• Testing guidelines are being established as part of the IT-DR methodology. As per the Action Plan noted in Recommendation 4, a training program will be developed and provided to relevant stakeholders. • Timing: May, 2009