APPENDIX 1

DISASTER RECOVERY PLANNING FOR CITY COMPUTER FACILITIES

March 2008

TORONTO Auditor General's Office

Jeffrey Griffiths, C.A., C.F.E.
Auditor General
City of Toronto

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction

Many governments and other large organizations are developing contingency plans in the event a disaster disables corporate computer systems. Events such as the September 11, 2001 terrorist attack on the World Trade Center, the 2003 Northeast Blackout, which left 50 million people without power throughout North America, and Hurricane Katrina have served as a reminder of the importance of developing alternate methods of maintaining critical information technology resources in the event of a disaster. The ability to recover City information systems quickly is critical to public health, safety and the ongoing provision of City services.

What is an Information Technology Disaster Recovery Plan?

An Information Technology Disaster Recovery Plan is a plan for duplicating computer operations after a disaster prevents the use of a computer facility normally used to support critical City business operations.

The purpose of this audit is to provide a snapshot of planning efforts in the event a disaster strikes City computer facilities

Because the City's information technology disaster recovery planning is currently in progress, and has been for a number of years, the purpose of this audit is to provide a snapshot of what the City has accomplished and what work remains to be completed in preparing contingency plans in the event of a disaster.

Conclusion – the City has considerable work to complete before it can consider itself prepared for a disaster

We concluded that the City is not yet prepared in the event a disaster disables City information technology infrastructure. Management is working on improving its ability to deal with a situation where computer facilities become inoperable for an extended period. Management estimates that based on recent efforts, in the event of a computer disabling disaster, restoration of the City's email system and financial system would still take two to three weeks. According to management, these specific systems are targeted in the Disaster Recovery Plan to be able to be restored within two to three days by the end of 2008. However, other key systems will not be able to be recovered until more progress is made on the Disaster Recovery Plan.

Divisional efforts are currently underway however they are not coordinated with other City divisions or with the City's Agencies, Boards and Commissions

Several disaster recovery initiatives are currently underway. However, these initiatives are being undertaken in individual divisions and are not being coordinated at the Corporate level. High-level corporate coordination of disaster recovery plans including the City's Agencies, Boards and Commissions have not been initiated.

As part of our review, we benchmarked City of Toronto Disaster Recovery plans with other government agencies. Our benchmarking results indicate that the City is at a similar stage in its information technology disaster planning and preparedness as many other government organizations. The results of our benchmarking are detailed in Exhibit 3 of this report.

The City has a responsibility to maintain critical services in the event of a disaster

In the event of a disaster, the City of Toronto has a responsibility to maintain critical City services to its residents. These critical services include:

1. Information technology systems supporting services provided by the City's police, fire, traffic control and emergency services;

2. Systems operating City water and wastewater treatment facilities, intake and/or effluent structures, pumping stations and chlorination stations; and

3. Business systems including financial and communication systems that provide management support.

The coordination of City emergency response teams, the coordination of activities with representatives from other agencies that play a key role in an emergency and carrying out ongoing emergency management program activities is crucial.

Ontario Emergency Plans Act requires the City to ensure information technology resources are in place in a disaster

The *Ontario Emergency Plans Act* requires the City of Toronto to plan for disasters and emergencies such as a severe storm, a large fire or a transportation emergency. This requirement compels the City to ensure the necessary information technology resources are available to support the City of Toronto's Emergency Response Plan during a disaster or emergency. A comprehensive disaster recovery plan reduces the risk of non-compliance with legislation and City by-law requirements related to government services.

Previous Auditor General's report related to Management of Information Technology Assets

In January 2006, the Auditor General issued a report on the Management of Information Technology Assets that included concerns related to general oversight and City-wide direction and expressed the need for an information technology governance review. The City contracted with IBM to conduct a governance review and in October 2006 IBM issued their report. Since receiving the IBM report the City has initiated implementation of the recommendations in the IBM Information Technology Governance and Transformation report.

Significant efforts are required to prepare the City in the event of a computer facility disabling disaster

Implementation of the IT Governance and Transformation Project is still underway and although management efforts have been directed toward strengthening the governance framework, a number of important issues related to disaster recovery remain outstanding. Key among these issues is the coordination of disaster recovery programs with the City's Agencies, Boards and Commissions.

There has been some progress in implementing a corporate oversight framework over the disaster recovery planning process

Outcomes from the IT Governance and Transformation Project, such as a corporate governance model and action to consolidate computer equipment in fewer locations will have a direct impact on disaster recovery planning for City computer facilities. Understandably, a governance exercise of this nature is complex and requires time. To date there has been limited progress in implementing a corporate framework related to the City's disaster recovery planning process.

Our report contains seven high level recommendations

Our report contains seven high level recommendations relating to the development of disaster recovery plans. These recommendations centre on the need to:

- Develop a formal protocol with the Agencies, Boards and Commissions related to collaborating on information technology disaster recovery planning and preparedness;
- Implement a City-wide business continuity planning program policy outlining roles and responsibilities, resource requirements, training requirements, simulation and plan maintenance schedules;
- Establish an accountability framework and reporting protocol for the Chief Information Officer to report to the Business Advisory Panel on information technology disaster recovery planning and preparedness;
- Provide staff with training related to Information Technology Disaster Recovery Planning and Preparedness; and
- Ensure City-wide computer related backup and storage procedures comply with appropriate standards and practices.

A City-wide process is needed to identify critical systems

The City should establish a process first to ensure management reviews all computer facilities located throughout the City to determine the information technology resources to include in an Information Technology Disaster Recovery Plan.

Disaster recovery is costly, lengthy and difficult to address without a proper plan

Under the best of circumstances, implementing a recovery strategy when computer resources become inoperable can be a costly exercise. Without a plan, disaster recovery becomes unnecessarily costly, lengthy and difficult to resolve. There is a requirement for management to evaluate an acceptable level of risk in disaster planning and at the same time ensure that disaster recovery planning and preparedness minimize that risk.

BACKGROUND

What is a computer facility disaster?

A computer facility disaster is any event causing a significant disruption in computer operations for an extended period. Such a disaster may be the result of natural events such as a hurricane or the result of human intervention such as the September 11, 2001 terrorist attacks on the World Trade Center in New York City.

City computer facilities include "data centres" with a high concentration of computer equipment networking with multiple information systems, divisions and smaller divisional computer systems.

Quick response to a disaster is dependent on the City's planning and preparedness efforts

Responding to a disaster requires an immediate and coordinated response by a diverse group of normally independent organizations, vendors and City divisions. A swift and effective response requires functions to work together in a planned, coordinated and synchronized manner.

The City's timely, effective and efficient response is dependent on planning and preparedness efforts. Proper planning and preparedness ensures business continuity and protects the health, safety and welfare of City residents.

What is an IT Disaster Recovery Plan?

An Information Technology Disaster Recovery Plan is a plan for duplicating computer operations after a catastrophe or disaster prevents the use of computer facilities normally used to support City business. A disaster recovery plan includes actions designed to ensure critical information systems are activated at an alternate site and required business continuity information is available when needed in the event of a disaster.

Why prepare Information Technology Disaster Recovery Plans?

In the event of a disaster, the City has a responsibility to maintain the flow of City services to its residents. Management is responsible for ensuring the health, safety and welfare of City residents including the need to deliver essential services in the event of a disaster. Information systems supporting Public Health, Police Services, Fire, Emergency Medical Services, Transit Commission and Social Services are examples of where citizen health, safety and welfare may be compromised if information systems are not available for an extended period.

The Ontario Comprehensive Emergency Management Program requires that the City have a disaster plan. A comprehensive and complete plan includes restoring critical information technology systems such as communication systems in an emergency.

Potential regulatory, legal and operational costs of $5 million for 24 hour outage and $158 million for delays exceeding one month

There are also negative regulatory, legal and financial consequences. In a business impact study conducted by SunGard Availability Services for the City's Corporate Information and Technology Division, estimated losses from potential regulatory, legal, operational costs and potentially delayed or lost revenues were in the range of $5 million after 24 hours to $158 million if the delay exceeds one month.

Recent disasters have reminded organizations to recognize the value of being able to recover information systems quickly

Governmental organizations have always been aware of the risks associated with disasters. However, recent disasters have reminded organizations of the need to prepare in advance for the possibility of a disaster. Organizations are taking action in advance to prepare for the potential of a disaster.

Canada is not an exception when it comes to disasters. For example, the City of Toronto and many other communities throughout North America experienced a hydro blackout, which left 50 million people without power.

Generally accepted practices for disaster recovery and business continuity planning

The business continuity profession has published generally accepted practices for business continuity through the efforts of several organizations worldwide. Notable among those organizations are the Disaster Recovery Institute and the Business Continuity Institute.

The Disaster Recovery Institute and the Business Continuity Institute developed and adopted 10 subject areas of Professional Practices for Disaster Recovery and Business Continuity Planners as follows:

Industry experts agree that organizations should focus on 10 specific subject areas when developing disaster recovery plans

Table 1:

Professional Practice Areas for Business Continuity Planners

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Develop Business Continuity Strategies
5. Emergency Response Operations
6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Communications
10. Coordination with Public Authorities

Industry experts agree that organizations should focus on these ten subject areas when developing disaster recovery and business continuity plans.

Exhibit 1 attached to this report provides a more detailed explanation of the 10 areas.

In 2001, City external auditors reported a lack of computer system recovery plans

In 2001, the City's external auditors reported that the City did not have a formal organization-wide recovery plan for critical systems in the event of a computer-related disaster.

The City's external auditors reported: *"The City's reliance on information technology continues to increase. We noted however, that the City has not yet developed a formal, organizational-wide, recovery plan for critical systems in the even of a computer-related disaster. In the event of a disaster, the City would have to carry out ad hoc recovery procedures thereby increasing the risk of significant disruption to the City's operations."*

Some changes have been made to improve availability in a disaster

A 2006 update by the City's external auditors indicated that: "*We recognize that the City obtained a completed Business Impact Analysis (BIA), which will assist in determining minimum recovery timeframes for critical business systems. The next phase in this process will be to develop the plan to meet the requirements determined by the BIA. We support the City's initiatives in this area and suggest that a Full Disaster Recovery Plan be put in place*."

Since then, several projects to improve the City's ability to recover from an information technology disaster have been undertaken. Exhibit 2 attached to this report includes additional detail for certain of these projects. As well, Emergency Management Services and the Homes for the Aged Division are in the process of implementing an information technology disaster recovery plan for their respective computer facilities.

The City's main computer data centre facility has undergone changes to improve the availability of information technology services in a disaster. Replication and synchronization of computer equipment, redundant internet and power supply sources, standby diesel generators and fire protection systems are examples of steps taken to improve availability in the event of an extended service disruption.

With these measures now in place, the Corporate Information and Technology Division continues to work toward implementing a disaster recovery plan if the City's main data centre becomes inaccessible or inoperable.

The City still has considerable work to do before a workable information technology disaster recovery plan is in place

Currently underway are actions related to selecting information technology recovery options, confirming division recovery priorities and developing appropriate recovery procedures for critical information systems supported by the Corporate Information and Technology Division. Toronto Water and Corporate Information and Technology Division have partnered to construct a new data centre that will serve as both Toronto Water's new primary computer facility and the alternate site for use if the City's corporate computer facility is not available for an extended period. The infrastructure necessary to support critical corporate information technology systems at this alternate site is complete.

The information technology unit for one of the City's Divisions has also initiated an information technology disaster recovery project to identify information systems in use and the recovery priority for the Division. This initial step is complete with further action on hold pending the outcome of the information technology governance and transformation project now underway.

Management has completed tasks related to the first three subject areas listed above in Table 1 and is working on the fourth subject area.

City efforts to develop disaster recovery plans are through individual divisional initiatives rather than a coordinated City-wide approach involving the many information technology facilities and resources throughout the City.

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

Why we conducted this review

In 2004, the Auditor General's Work Plan included an audit of information technology disaster recovery planning and preparedness. In the early stages of the audit we determined that city staff had only recently initiated work in disaster recovery planning. Consequently, we deferred further work until such time as an audit would yield meaningful results. This report presents the results of the audit deferred in 2004.

This audit identifies challenges and gaps in the planning and preparedness process and recommends steps to improve the process. The overall question addressed in this review is:

"How effective are the City's current planning and preparedness efforts in restoring information technology services in the event a disaster prevents extended use of City computer facilities?"

What were the objectives of the audit?

Our objectives were to review the working relationship between the City and the Agencies, Boards and Commissions in relation to information technology disaster recovery planning, City Disaster Recovery policies and procedures, and the role of the Information and Technology Division in creating, coordinating, and overseeing disaster recovery planning initiatives for City computer facilities.

Specific objectives were to determine:

- the adequacy of current corporate governance and coordination of disaster recovery planning for the City's computer facilities;
- compliance with related laws, rules and regulations;
- compliance with generally accepted standards for disaster recovery planning and management for computer facilities; and
- completeness of computer facility disaster recovery plans, and related policies and procedures.

Our audit included three main components:

Our audit covered disaster recovery planning and recovery activities through to November 2007 and included three main components:

A comparison with criteria and activities established by related authoritative bodies

1. A comparison with planning criteria and activities recommended by the:

   - Disaster Recovery Institute and Business Continuity Institute;

   - National Institute of Standards and Technology for the US Department of Commerce "Contingency Planning Guide Information Technology Systems"; and

   - Information Systems Audit and Control Association Guidelines for "Business Continuity Plan Review from an IT Perspective."

A review of City disaster recovery plans

2. A review of information technology disaster recovery plans prepared by the City and related documents including reports from the Information Technology Governance and Transformation Project, a Business Impact Assessment Report, and the Business Impact Analysis prepared on behalf of the Corporate Information and Technology Division.

A review of the status of other governmental agencies in relation to disaster recovery planning

3. A review of the planning and preparedness status of other governmental computer facilities including:

   - City of Calgary;
   - County of Los Angeles;
   - Greater London Authority (UK);
   - State of Colorado; and
   - United States Department of Homeland Security

This report does not address facility-level or organizational contingency planning except for those issues required to restore computer data centre facilities and their processing capabilities. In addition, the report does not address contingency planning for City divisional business processes. That topic would be more appropriately addressed in a review of the City's planning and preparedness process for individual divisional business continuity.

We conducted this audit in accordance with generally accepted government auditing standards

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DETAILED AUDIT RESULTS AND RECOMMENDATIONS

A. A FORMAL PROTOCOL WITH AGENCIES, BOARDS AND COMMISSIONS IS REQUIRED

Information technology governance review recommended by the Auditor General in 2006

In January 2006, the Auditor General issued a report on the Management of Information Technology Assets that included concerns related to general oversight and governance of information technology. The 2006 report expressed the need for an information technology governance review. Management contracted with IBM to complete the recommended governance review and in October 2007 the final report from IBM was completed. Management has initiated steps to implement recommendations included in the report.

The Auditor General, in the 2006 report, also suggested that the review of the governance structure include the City's Agencies, Boards and Commissions. Management agreed to consider this after the governance review within the City was complete.

In several reports issued by the Auditor General's Office in the past and included in this report, is the need for a closer working relationship between the City and its Agencies, Boards and Commissions.

Opportunities exist for improving efficiencies through knowledge sharing

Opportunities exist for improving efficiencies through coordinating disaster recovery efforts, sharing of knowledge and use of common tools related to information technology disaster planning and preparedness.

No formal communication or coordination with the Toronto Police Service

For example, we noted that although the Toronto Police Service uses the City's main data centre facility as a recovery site there are no formal lines of communication and coordination with the City to ensure recovery strategies and supporting resources are synchronized. Lack of coordination increases the risk that efforts are either duplicated, overlap or conflict.

A more formal relationship will ensure each organization's planning process is properly linked and coordination and cooperation related to an extended interruption in computer services is effective in maintaining delivery of critical City services.

Recommendation:

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.

B. A DISASTER RECOVERY AND BUSINESS CONTINUITY PROGRAM SHOULD BE DEVELOPED

Toronto's Emergency Plan requires City divisions employ standard business continuity planning principles

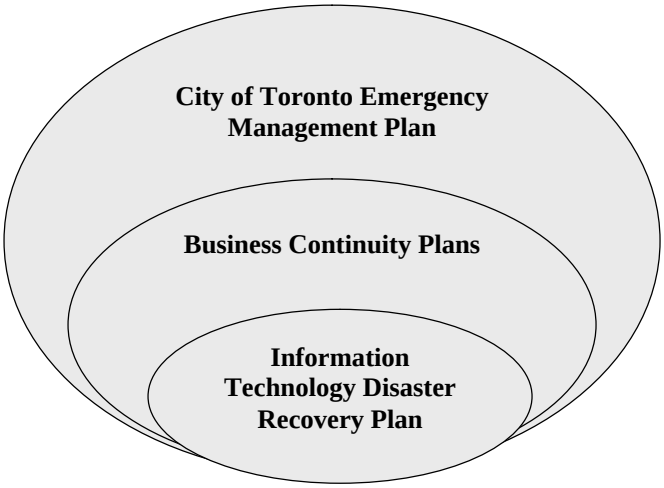
The City of Toronto's Emergency Plan establishes the framework that ensures the City is prepared to deal with a disaster. It is the process followed by the City to mobilize resources in the event of an emergency.

Included in the Emergency Plan is the requirement for City divisions to employ standard business continuity planning principles to ensure continuity of essential services. Divisions are responsible for taking the lead in preparing and maintaining business continuity plans.

Since there is an inherent relationship between computer information systems and the business processes they support, the generally accepted practice is to develop and implement information technology disaster recovery plans within the context of the broader business continuity plan. The diagram below illustrates the relationship between the three plans within the global Emergency Management Plan. High-level communication and coordination is required for the plans to work as one in the event of a disaster.

Figure 1

Relationship of Information Technology Disaster Recovery Plan and the City's Emergency Management Plan



Periodic simulation, testing and updating is required in order for disaster recovery plans to be useful

Regular simulation, testing and updating of division plans is required in order to be effective. The City's overall Emergency Management Plan assigns responsibility for coordinating disaster recovery plans to the Corporate Office of Emergency Management. The Emergency Management Plan requires divisions to review and revise plans and support the operations of the City's Office of Emergency Management. Divisions are also required to periodically test business continuity plans and keep them current.

Because of the critical relationship between computer systems and the business process they support, we requested business continuity plans from City divisions. We were unable to obtain a complete, comprehensive and current business continuity plan. Plans either did not exist, did not include what business processes would be invoked when computer services were interrupted for an extended period, or were not current.

A formal City-wide disaster recovery and business continuity program is needed

Coordination between business continuity plans and information technology disaster recovery plans ensures recovery plans and supporting resources do not work at cross purposes, overlap or duplicate efforts.

A formal program to support City-wide business continuity planning and a coordinated approach involving both information technology staff and division operational staff is required.

Recommendation:

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.

C. INFORMATION TECHNOLOGY DISASTER RECOVERY PLANNING PROCESS SHOULD INCLUDE PERIODIC REPORTING

Disaster recovery is part of managing information technology resources

Planning for computer related disaster recovery is part of managing the City's information technology resources. Recent changes made by the City's Governance and Transformation Team provide an opportunity to improve disaster recovery oversight.

A Business Advisory Panel to oversee management of the City's information technology resources has been established

In redesigning the governance model for information technology services management established a Business Advisory Panel chaired by the City Manager. The mission of the Business Advisory Panel is to provide strategic direction, establish business priorities and guide the City's investment in information technology.

Strategic direction for information technology disaster recovery planning rests with the Chief Information Officer

The new governance structure assigns responsibility for setting strategic direction for computer system business continuity planning to the Technology Risk Management and Information Security Unit. This unit reports to the City's Chief Information Officer. Placing this responsibility in this Unit is consistent with other leading organizations where disaster recovery planning is now a priority in the overall risk management and corporate governance strategy.

Reporting relationship between the Chief Information Officer and the Business Advisory Panel needs to be established

Given the oversight responsibility of the Business Advisory Panel, a regular reporting relationship should be established that ensures the Chief Information Officer reports to the Business Advisory Panel on City-wide disaster recovery planning and preparedness for information technology systems.

Periodic reporting will ensure that planning and preparedness efforts are consistent with and support the long-term direction of the City in its ability to recover from a disaster affecting City computer facilities.

Recommendation:

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.

D. TRAINING AND GUIDANCE IN PREPARING INFORMATION TECHNOLOGY DISASTER RECOVERY PLANS ARE NEEDED

The City operates in a complex information technology environment

The City operates in a complex environment with various management groups responsible for delivering information technology services, multiple computer facilities and numerous information systems. Information systems controlled by one division may be used by another division and could be supported by yet a third division.

Coordinated approach ensures consistent, effective and efficient plans

Proper training, management oversight and a coordinated systematic approach ensure disaster recovery plans are implemented in an effective and efficient manner.

Plans were not consistently prepared with best practices in mind

Information technology disaster recovery plans provided by divisions responsible for their own computer resources were not consistently prepared in accordance with best practices. Best practice disaster recovery plans require divisions to provide information on whom to contact in a disaster, when to contact them, where to contact them, what is expected of them, and how they are to accomplish their respective responsibilities. Plans often did not deal with who is responsible for what, did not include the location of an alternate site to continue operations if their current computer facility becomes unavailable, or were not current.

Plans often did not answer the who, what, where questions

Recommendation:

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.

E. BACKUP AND OFFSITE STORAGE PRACTICES SHOULD BE STRENGTHENED

A key component of any disaster recovery plan is a provision for offsite storage of City data

A key component of any disaster recovery plan is an offsite location for storage of computer media containing City data. The offsite storage location should be far enough away that a single event will not result in the destruction of both the computer facility used to support daily operations and the offsite storage location. However, the offsite location should not be so far away as to discourage the regular rotation of computer media.

Some divisions do not practice appropriate backup and offsite storage procedures

While the Corporate Information and Technology Division stores backup media offsite, there are divisions that store current computer media and backup media in the same building. We also noted divisions did not always maintain a complete record of the location of backup computer media. As well, divisions are not always aware of existing arrangements the City has with storage service providers and the opportunity for them to participate in these services.

If appropriate backup and offsite storage procedures are not in place and followed, data required to restore computer systems will not be available to maintain critical City services in the event of an extended interruption.

Recommendation:

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 the outside service provider.

F. INFORMATION TECHNOLOGY DISASTER RECOVERY PLANS SHOULD BE TESTED PERIODICALLY

Periodic simulation and testing required

Technology disaster recovery plan simulation and testing is critical to ensure the plan is effective and practical. Simulation and testing is useful in identifying and addressing deficiencies in the plan. Testing also aids in assessing the ability of the recovery team to implement the plan quickly and effectively.

Divisions are not testing their recovery capability

While the Corporate Information and Technology Division has disaster recovery testing in place for the outsourced mainframe applications there are divisions that are not testing their recovery capability in the event of an extended interruption in computer services.

Experts agree there is no value in an untested plan

There is no formal requirement for divisions to test and update their information technology disaster recovery plans. Guidelines and standards related to how and when simulation and testing should be conducted are not provided to divisions. Disaster recovery experts agree that there is no value in an untested plan. It is likely that an untested plan will not work well when a real disaster occurs.

In order to properly safeguard City information technology assets, disaster recovery plans should be periodically tested to ensure they remain practical and effective in an extended outage. The City will spend in excess of $7 million over the next five years to implement technology disaster recovery plans. Without testing recovery plans on a regular basis, the City will not receive the benefit of the intended purpose and value of having such plans in place.

Recommendations:

6. **The City Manager, in consultation with the Chief Information Officer, direct divisions to test information technology disaster recovery plans on a regular basis.**

7. **The Chief Information Officer develop disaster recovery testing guidelines and provide training necessary to ensure cross-divisional consistency.**

CONCLUSION

Conclusion - The City has much work to do to protect and maintain critical computer services in the event of a disaster

We began our review by asking, "How effective are the City's current planning and preparedness efforts in restoring information technology services in the event a disaster prevents extended use of City computer facilities?"

During the early stages of our review, it became evident that much work is needed in order to protect and maintain critical City information technology resources in the event of an extended service disruption or disaster. As the City's Information Technology Governance and Transformation Project unfolds, management should place a high priority on addressing the challenges and gaps identified in disaster recovery planning and preparedness.

With adequate planning and preparedness, the City will be in a better position to minimize the negative effects of extended computer service interruptions and maintain critical public services in the event of a disaster.

Exhibit 1

Ten Subject Areas of Professional Practice for Business Continuity Planners
Adopted By Disaster Recovery Institute (DRI) and Business Continuity Institute (BCI)

	Area	Brief Description
1	Project Initiation and Management	Establish the need for a Business Continuity Plan (BCP) including obtaining management support and organizing and managing the project to completion within time and budget limits.
2	Risk Evaluation and Control	Determine the events and environmental surroundings that can adversely affect the City and its facilities with disruption as well as disaster, the damage such events can case, and the controls needed to prevent or minimize the effects of potential loss. Provide cost benefit analysis to justify investment in controls to mitigate risks
3	Business Impact Analysis	Identify the impacts resulting from disruptions and disaster scenarios that can effect the City and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.
4	Develop Business Continuity Strategies	Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective while maintaining the City's critical functions.
5	Emergency Response and Operations	Develop and implement procedures for a response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Centre to be used as a command centre during an emergency.
6	Developing and Implementing Business Continuity Plans	Design, develop and implement the Business Continuity Plan that provides recovery within the recovery time objective.
7	Awareness and Training Programs	Prepare a program to create corporate awareness and enhance the skills required to develop, implement, maintain and execute the Business Continuity Plan
8	Maintaining and exercising Business Continuity Plans	Pre-plan and coordinate plan exercises and evaluate and document plan results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the City's strategic direction. Verify that the Business Continuity Plan will prove effective by comparison with suitable standards, and report results in a clear and concise manner.
9	Public Relations and Crisis Communication	Develop, coordinate, evaluate and exercise plans to communicate with the media during a crisis. Develop, coordinate, evaluate and exercise plans to communicate with management during crisis. Ensure all stakeholders are informed on an as-needed basis.
10	Coordination with Public Authorities	Establish applicable procedures and policies for coordinating response, continuity, and restoration activities with local authorities while ensuring compliance with applicable statutes or legislation.

Exhibit 2

Past and Proposed Projects to Improve the City's Disaster Recovery Preparedness for Information Systems			
Division	**Project Name**	**$$$ (million)**	
		Actual	**Planned**
Current Projects			
Emergency Management & Fire Services	Headquarters Power Supply		$3.1
Information & Technology	Technology Disaster Recovery Plan		$7.9
Information & Technology	Network Upgrade Disaster Recovery Plan	$2.4	$4.5
Technical Services	Information Technology Disaster Recovery Plan	$0.6	$0.7
Completed Projects			
Information & Technology	Business Impact Analysis & Strategy Options performed by SunGard Availability Services	$0.4	$0.4
Information & Technology	Network Upgrade – 2001 Disaster Recovery Plan	$0.9	$0.9
Policy, Planning, Finance & Administration	Business Impact Analysis & Risk Assessment	$0.389	$0.7

Exhibit 3

Summary Results Summary Review of Audit Reports from Government Agencies Related to Information Technology Disaster Recovery Planning and Preparedness		
Government Agency	**Area Reviewed**	**Comments**
Greater London Authority (UK)	Disaster Recovery Planning – June 2007	• Overall, Disaster Recovery well managed • Disaster Recovery site is well managed • Disaster Recovery plan tested on a bi-annual basis • Improvement in the control framework needed to ensure plan documentation is updated, contact list remains current, and completeness of Test Log records
State of Colorado	Mainframe Disaster Recovery – Performance Audit – January 2007	• The Office of Information Technology is not ensuring departments have developed disaster recovery plans for systems on the mainframe computer • Disaster recovery plans were found to be inadequate • The disaster recovery plans were not adequately tested • Poor coordination of tests performed • Disaster recovery policy needs updating
Fairfax County, Virginia	Datacentre Disaster Recovery Audit Report – September 2006	• Comprehensive Disaster Recovery Plan in the process of being developed o Plan did not include all applications o Business Impact Analysis incomplete o Goals and objectives for testing were not defined
City of Calgary	IT Business Continuity Plans – May 2005	• No corporate wide business continuity plans in place for information technology • Disaster recovery plans for critical information systems were inadequate • Disaster recovery plans previously developed were not maintained
US Department of Homeland Security	Disaster Recovery Planning for DHS Information Systems – May 2005	• Information technology disaster recovery sites were not prepared to prevent service disruptions • A high percentage of disaster recovery planning documents were deficient and in some cases not finalized

		• There is no program in place to provide an enterprise-wide disaster recovery solution
Los Angeles County, California	Review of Internal Services Departments Disaster Recovery Plan for its Mainframe and Network Computer Operations – June 2002	• County-wide system recovery priorities do not exist to assist departments in coordinating their disaster recovery plans • A county-wide Business Impact Analysis does exist • The Disaster Recovery Plan is not comprehensive