SUBJECT: Disaster Recovery Plan Project Update (FCS06033) (City Wide)

RECOMMENDATION:

That report FCS06033 “Disaster Recovery Plan Project Update”, be received for information.

EXECUTIVE SUMMARY:

This report provides an update on the City’s Information Technology Disaster Recovery planning activities.

The absence of a Disaster Recovery Plan was noted in the 2004 external auditor (Grant Thornton) findings to be an item of high risk to the City. In order to address that risk, the IT Division developed a preliminary plan in 2005. This version of the plan targets three critical applications and can be used by Information Technology (IT) staff to restore these systems in the event of a disaster. It is expected that a more comprehensive plan will be developed as the disaster recovery project proceeds and further analysis work is completed.

The main goal of a Disaster Recovery Plan is to minimize the impact on computer systems and to mitigate costs associated with the recovery of such systems in the event of a disaster.
The City’s Disaster Recovery Plan is a document that outlines a process for the recovery of critical applications and data, should such an event, result in destruction or loss of the City’s data centre.

The City currently operates a single data centre where critical applications (e.g., e-mail, Peoplesoft) operate along with the core components of the City’s voice and data network. A Disaster Recovery Plan will assist the organization in restoring these critical applications. However, relying on a single data centre increases the risk to the City. As the plan exists today, significant time and effort would be required to rebuild the City’s data centre if it were to suffer damage or total destruction. Therefore, upcoming phases of this project will explore options for establishing an alternate data centre site. This facility would act as a back-up to the existing primary data centre and would enable the City to recover critical computer systems in a timely manner should the operation of the primary centre be impacted by a disastrous event.

**BACKGROUND:**

For the purposes of Disaster Recovery planning, a disaster is:

“Any interruption to computer operations that prompts a decision to go to the off-site recovery location (alternate Data Centre). Interruptions can include the loss of infrastructures that are not the property of the City of Hamilton but on which the City of Hamilton depends. This can include: fibre, power grids, telephone switching centres, cell and wireless transmission sites within a ten (10) mile radius of the facility.”

Recent disastrous events occurring in New Orleans and other locations around the world have reminded us of the importance of protecting our assets and maintaining the ability to effectively respond to an emergency situation. The City’s annual emergency exercise conducted in 2005 involved the evacuation of an area where the City’s current data centre is located. If that were an actual emergency, it is likely that the City’s computer systems would have been rendered inoperative. On November 9, 2005, the City suffered significant damage caused by a powerful tornado. These events serve as a reminder that a comprehensive and tested Disaster Recovery Plan is essential in maintaining the delivery of critical services to public.

A Disaster Recovery Plan provides guidelines and instructions for Information Technology staff to follow in the event of a prolonged disruption of computer services. This ensures critical applications can be brought on-line as efficiently as possible.

The 2004 findings of the external auditor (Grant Thornton) reported that the City of Hamilton did not have a documented and tested Disaster Recovery Plan to support the organization in a successful recovery of its’ systems, networks and applications in the event of a disaster. Lack of a documented and tested Disaster Recovery Plan would make it extremely difficult for the City of Hamilton to successfully recover its’ systems, networks, applications and data in the event of a disaster affecting IT systems. As a result, it was recommended that the City of Hamilton prepare and document a Disaster
Recovery Plan for critical systems and that the plan be tested on, at least, an annual basis.

Disaster Recovery planning is a corporate initiative. To create a comprehensive Disaster Recovery Plan, an analysis of all existing computer business applications must be completed. This analysis will determine the impact to the organization if these applications are not available for an extended period of time. An analysis of this type takes a substantial amount of time and effort. Therefore, to achieve some value quickly and to lower the immediate risk, Information Technology staff drafted a useable plan in 2005 (Appendix A to report FCS06033 lists the Table of Contents for this Plan).

Key assumptions in the existing Disaster Recovery Plan are:

- The plan is designed to define and test the procedures necessary to recover from the “worst case” destruction of the City of Hamilton’s computer Data Centre. This includes Information Technology offices in close proximity to the Data Centre.
- The “worst case” destruction assumes the loss of the data centre facility located at 55 York Boulevard, 6th floor.
- Although the plan is designed for “worst case”, inherent in the plan strategy is the ability to recover up to the most minor interruption.
- The plan is based upon a sufficient number of staff not being incapacitated to implement and affect recovery. The level of detail of the plan is written for staff experienced in the City’s computer services. Development, testing and implementation of new technologies and applications would be halted such that all resources are available to recover existing critical production processing.
- Off-site inventory and equipment is considered to be the only resource with which to recover computer processing. Items at the original site are not expected to be salvageable and used for recovery.
- An alternate site (back-up computer facility) in which to establish recovery of computer processing is necessary. Time frame requirements to recover computer processing are significantly less than estimated times to repair/reconstruct a data centre on an emergency basis.
- The computer facilities at the alternate site are not impacted by any disaster which may interrupt computer operations at 55 York Boulevard, 6th floor.

To assist the existing Disaster Recovery Plan, the IT Division currently performs system back-ups, on a regular basis, maintains documentation on recovery procedures and stores back-up media at an off-site location. In the event of a system failure or data loss, the back-up media can be used to restore a system to its’ normal functioning state. In addition, various levels of redundancy are built into the network infrastructure, servers, and applications. Redundant capabilities allow an application to continue running by using a readily available back-up server.

It is important to note that the existence of a plan does not guarantee a quick restore. If a disastrous event were to occur that resulted in total destruction or loss of the City’s data centre, significant effort would be required to rebuild a site. Therefore, to further mitigate the risk of a data centre disaster, most organizations have a pre-built site, or access to an alternative site, which is available immediately in order to restore and run
critical applications. Redundant equipment is normally located at a back-up location. Since the City does not currently have a back-up site, its’ current redundancy capabilities would be lost if the existing data centre were to sustain damage.

The City’s existing plan is limited to three key areas of technology. Therefore, further analysis need to be completed. The plan needs to be tested and a back-up data centre location needs to be considered. These additional steps will ensure that the plan is complete and will further minimize the risk to the City.

**ANALYSIS/RATIONALE:**

The City’s disaster recovery planning initiative is to be carried out in 3 phases:

Phase 1 - A plan was developed that addresses three computer systems deemed to be mission-critical to the corporation.
Phase 2 - Scheduled to begin in 2006, will include a business impact analysis exercise identifying additional critical applications that will be included as part of a revised Disaster Recovery Plan.
Phase 3 - Proposes to establish an alternate data centre location and will ensure that processes are developed to test the plan on an annual basis.

**Phase I – Establish Usable Plan**
The City’s IP phone system, the corporate e-mail system and the Financial and Human Resource Peoplesoft application modules were included in this phase.

The phone system and corporate e-mail are considered to be critical communication tools. In the event that a disaster occurs in our City, the Emergency Operations Centre relies heavily upon both phones and e-mail to conduct their activities. Recovery of these systems is required within a twenty-four hour timeframe. It has been determined that both the Financial and Human Resource applications of Peoplesoft should be available to City staff within forty-eight hours of a disaster event. Important data is stored electronically in the Peoplesoft system and payroll could be processed only once without access to these electronic records. With Peoplesoft out-of-service, payments to vendors would be delayed resulting in late payment charges and possible suspension of goods and/or service delivery.

This phase has delivered a useable plan that can be executed by City staff in the event a disaster that impacts our existing data centre.

In order to meet the 24 and 48 hour recovery time requirements for the critical Phase I applications, an alternate data centre site must be available. Without this site, IT Services would have to locate an alternate data centre, prepare the site with proper air conditioning, electrical supply, network cabling, security, etc., and order and install computer equipment, all prior to recovering any computer applications or data. This leaves City staff without phones, e-mail and computer applications for that length of time. In the event of a disaster, the cost to the organization could be in the range of millions of dollars and have a significant impact on our ability to deliver services to the public.
To have the IP Telephony and corporate e-mail systems back up and running in 24 hours, all equipment and software must be pre-installed and ready to use. As the plan exists today, this recovery time is not possible. Without additional equipment available at a backup site, it would take approximately 4-6 weeks for the critical applications to be completely restored and available for use.

The absence of an alternate data centre site makes it extremely difficult to test, validate, and maintain the existing plan.

The following equipment (at an estimated one-time cost of $500k) would be required at a backup site to allow recovery of e-mail, Peoplesoft, and telephone services within a 24 – 48 hour period:

- E-Mail Server
- Peoplesoft Servers and Storage
- IP Phone System Equipment
- Air Conditioning Unit
- Additional Power and Wiring

It is expected that additional equipment will be required if other critical applications are identified in phase 2 of the project.

To date, the activities undertaken in this phase have been completed by internal IT staff at no cost.

**Phase 2 – Business Impact Analysis and Plan Review**

In Phase 2, $50,000 from the existing Disaster Recovery Capital Project budget will be used to complete a full Business Impact Analysis. This analysis will identify other critical computer applications by measuring the impact to the corporation, should an application be unavailable for an extended length of time. The existing Disaster Recovery Plan will be reviewed and updated based on the findings from the business impact analysis.

Equipment that is critical to the operation of the Hamilton Public Library system is also located in the City’s data centre. These systems are managed by the Library’s Electronic Services Team. The Library is currently developing a recovery plan and will, therefore, be participating in the business impact analysis exercise in this phase.

This phase will also explore options for establishing a permanent and reliable backup data centre site. Sharing the cost of building/furbishing an alternate data centre with an alternate Emergency Operations Centre is an option that will be investigated further at this stage. A report will be presented to Council outlining the results of the business impact analysis and will provide options and costs for a permanent backup data centre site.

The work in this phase is expected to begin in March of 2006 and be completed in late summer or early fall.
Phase 3 – Establish Permanent Backup Data Centre
Should Council wish to proceed with a back-up data centre, this phase will involve implementing a back-up site that can accommodate the operation of all critical applications as identified in Phase 2.

Disaster Recovery Plan Maintenance
It is important to recognize that Disaster Recovery planning is an on-going process, not a point in time exercise. As new computer applications are implemented or existing computer applications are enhanced, the Disaster Recovery Plan must be updated.

Not unlike the City of Hamilton’s Emergency Operations Plan, a Disaster Recovery Plan must be regularly validated by testing. Best practises recommend testing the plan at least once per year. A testing schedule will be developed and the first test of the completed plan will occur in 2006. Tests will expose inappropriate assumptions and weaknesses in the Disaster Recovery Plan. Improvements can then be made to the plan, so that when a real disaster occurs, critical services can be effectively and efficiently restored.

It is anticipated that upon completion of Phase 2, additional resources will be required to establish and manage a back-up data centre, to maintain an up-to-date Disaster Recovery Plan and to complete the required testing on an annual basis. Depending on the complexity of the plan, these costs could range from $100k - $200k per year. Detailed resources needs, will be outlined in a future report.

[ALTERNATIVES FOR CONSIDERATION:] This is an information report with no alternatives to consider at this time.

[FINANCIAL/STAFFING/LEGAL IMPLICATIONS:]

Financial Implications:
Disaster Recovery Plans not only require capital funding for initial set-up of an alternate data centre site, they require an annual operational budget to ensure the plan and equipment is maintained and kept up-to-date and to provide staff time to adequately test the plan. As with the Emergency Operations Centre, if testing is not done on a regular basis, the plan cannot be validated and there is no guarantee it will work when required.

A $50k Disaster Recovery capital program was previously established to assist in the development of a plan.

Staffing Implications:
IT Services staff will be required to plan, order, install, configure and operate the alternate site should one be established in Phase 3. Best practises recommend testing of the Disaster Recovery Plan to be done at least once per year. Tests can vary in scope, however, staff time will be required to plan and schedule the test, execute the test
and document the results. Frequent testing will highlight deficiencies in the Disaster Recovery Plan which must then be corrected.

Phase 2 of the project will require extensive consultation with all departments during the business impact analysis process.

**Legal Implications:**
There are no immediate legal implications. However, in the event of a disaster there are the following risks to consider:
- Possible implications for non-payment or improper payment of staff and vendors
- Withdrawal of vendor services
- Constituents unable to contact the City for services or inquiries
- Delays in receiving and processing revenues.

**POLICIES AFFECTING PROPOSAL:**
There are no policies affecting this proposal.

**RELEVANT CONSULTATION:**
All City departments have been asked to validate an inventory of computer applications. ITST (the Information Technology Strategic Team) has provided input and guidance to the current Disaster Recovery planning efforts.

The Emergency Operations Centre has read a draft of the plan and provided comments.

Senior Finance and Human Resources staff were consulted to determine the impact of losing the Peoplesoft application for an extended period of time.

Disaster Recovery Plans from other municipal and regional governments have been reviewed for content.

**CITY STRATEGIC COMMITMENT:**
By evaluating the “Triple Bottom Line”, (community, environment, economic implications) we can make choices that create value across all three bottom lines, moving us closer to our vision for a sustainable community, and Provincial interests.

Evaluate the implications of your recommendations by indicating and completing the sections below. Consider both short-term and long-term implications.

**Community Well-Being is enhanced. □ Yes □ No**

A Disaster Recovery plan implemented and maintained along with a backup data centre site, will ensure prompt recovery of critical systems in the event of a disaster. This will enable departments to deliver programs in a manner that supports the well-being of communities in the City of Hamilton.
Environmental Well-Being is enhanced. ☑ Yes ☐ No

A Disaster Recovery plan implemented and maintained along with a backup data centre site will ensure prompt recovery of critical systems in the event of a disaster. This will enable departments to deliver programs in a manner that supports the environmental well-being of communities in the City of Hamilton.

Economic Well-Being is enhanced. ☑ Yes ☐ No

A comprehensive Disaster Recovery Plan that can be used to promptly recover critical computer systems will help to maintain the economic well-being of the City should a disaster occur.

Does the option you are recommending create value across all three bottom lines? ☑ Yes ☐ No

Do the options you are recommending make Hamilton a City of choice for high performance public servants? ☑ Yes ☐ No

The existence of a disaster recovery plan will provide staff with the tools necessary to restore critical applications as efficiently and effectively as possible.
APPENDIX A
INFORMATION TECHNOLOGY SERVICES
DISASTER RECOVERY PLAN
PHASE I - TABLE OF CONTENTS

Preface

1.0 Plan Introduction
   1.1 Overview
   1.2 Mission and Objectives
   1.3 Disaster Recovery Plan Scope
   1.4 Responsibility
   1.5 Key Plan Assumptions
   1.6 Disaster Definition

2.0 Disruption Prevention Strategies
   2.1 Purpose
   2.2 Corporate Data Storage Policy
   2.3 Data Backup Process
   2.4 Network Redundancy Strategies (voice & data)
   2.5 Power Redundancy Strategies
   2.6 Computing Redundancy Strategies

3.0 Recovery Strategy
   3.1 Critical Time Frame
   3.2 Approach
   3.3 Escalation Plans
   3.4 Decision Points
   3.5 Impending Disaster Procedures

4.0 Disaster Recovery Organization
   4.1 Disaster Management Team
      4.1.1 Disaster Management Team Responsibilities
      4.1.2 Disaster Management Team Checklist
   4.2 Recovery Management Team
      4.2.1 Recovery Management Team Responsibilities
      4.2.2 Recovery Management Team Checklist
   4.3 Damage Assessment Team
      4.3.1 Damage Assessment Team Responsibilities
      4.3.2 Damage Assessment Team Checklist
   4.4 Hardware Installation Team
      4.4.1 Hardware Installation Team Responsibilities
      4.4.2 Hardware Installation Team Checklist
   4.5 Network & Communications Team
      4.5.1 Network & Communications Team Responsibilities
      4.5.2 Network & Communications Team Checklist
   4.6 Operations & Restore Team
      4.6.1 Operations & Restore Team Responsibilities
      4.6.2 Operations & Restore Team Checklist
APPENDIX A (continued)
INFORMATION TECHNOLOGY SERVICES
DISASTER RECOVERY PLAN
PHASE I TABLE OF CONTENTS

4.7 Applications & Software Team
   4.7.1 Applications & Software Team Responsibilities
   4.7.2 Applications & Software Team Checklist

5.0 Plan Administration
   5.1 Distribution of the Disaster Recovery Plan
   5.2 Training the Recovery Teams
   5.3 Testing the Disaster Recovery Plan
   5.4 Maintaining the Disaster Recovery Plan

6.0 Alert Procedures
   6.1 First Alert Notification Summary Procedures
   6.2 Initial IT Response Team Assessment Procedures

7.0 Recovery Process & Documentation
   7.1 Infrastructure Recovery Documentation
      7.1.1 Windows 2000 Server Installation Instructions
      7.1.2 Windows 2003 Server Installation Instructions
      7.1.3 Server Installation Checklist & Install Worksheet
      7.1.4 Veritas Install Instructions
   7.2 Telecommunications Recovery Documentation
   7.3 Application Recovery Documentation
      7.3.1 Microsoft Exchange Server Recovery Instructions
      7.3.2 Peoplesoft Financials Recovery Instructions
      7.3.3 Peoplesoft Human Resources Recovery Instructions

8.0 Appendices
   8.1 Vendor Contact List
   8.2 Network Schemata
   8.3 Infrastructure Inventory
   8.4 Applications Inventory
   8.5 Plan Distribution List
   8.6 Test Schedule
   8.7 Off-Site Recovery Box Inventory
   8.8 Team Call Lists
      8.8.1 Disaster Management Team Call List
      8.8.2 Recovery Management Team Call List
      8.8.3 Damage Assessment Team Call List
      8.8.4 Hardware Installation Team Call List
      8.8.5 Network & Communications Team Call List
      8.8.6 Operations & Restore Team Call List
      8.8.7 Applications & Software Team Call List