SUBJECT: Information Services - Disaster Recovery (FCS09017) (City Wide)

RECOMMENDATION:

a) That City staff be directed to proceed with Phase 3 of the Information Services (IS) Disaster Recovery Planning Project to build a backup data centre as part of the new Hamilton Public Library Waterdown Construction Project (approved by the Hamilton Public Library Board September 17, 2008); and

b) That project costs be charged to capital project 3500941906 (IS Construct a Disaster Recovery Facility).

EXECUTIVE SUMMARY:

This report addresses Item 3 from the Grant Thornton 2007 Audit Results report as presented to the Audit and Administration Committee – Item 7.1(a) May 21, 2008. In their audit results, Grant Thornton recommended that the City finalize the Disaster Recovery Plan as soon as possible.

The Information Services Division has developed an IS Disaster Recovery Plan that documents the processes for the recovery of critical business applications. The main goals of this Disaster Recovery Plan are to minimize the impact of a disaster affecting the City’s business applications, to mitigate recovery costs associated with the recovery of these applications and to allow the City to continue to provide services to the community following the disaster.
The IS Disaster Recovery Plan has proceeded in three (3) phases:

**Phase 1 – Develop Preliminary Disaster Recovery (DR) Plan** [complete]
Phase 1 was completed in 2005. It was based on the recovery of a limited number of core systems including the core network, IP telephone system, corporate e-mail and Finance and Human Resource systems. The deliverables from this phase were documented processes and configurations. Phase 1 included no computer hardware or backup data centre.

**Phase 2 – Complete Business Impact and Risk Assessments** [complete]
Phase 2 was completed in 2006. It involved input from all City Divisions under the direction of Disaster Recovery (DR) specialists. It provided an assessment of the risks affecting the City’s computer systems and produced a prioritized list of applications and detailed recommendations for their recovery in the event of a disaster. Based on the Business Impact Assessment, some applications must be recovered within four (4) hours and many applications must be recovered within twenty-four (24) hours of the declaration of a disaster.

The DR specialists recommended that the only way to ensure such short recovery times for many applications would be to implement a “hot site” – i.e., a backup data centre complete with functioning network and computer systems. Without a fully functional backup data centre, disaster recovery would start with either acquiring hardware or installing operating systems and applications on existing hardware. Neither option would meet the stated business requirements of four (4) to twenty-four (24) hours.

The report from the DR specialists recommended the implementation of a hot site at a City-owned facility.

**Phase 3 – Implement Revised Plan and Backup Site** [outstanding]
Phase 3 has not been completed. This phase acts on the recommendations of the DR specialists and the findings from the Grant Thornton 2007 audit to implement the full DR Plan, including the backup data centre.

This report deals with Phase 3 of the DR Plan, including the selection of a backup data centre site and the funding necessary to implement and maintain both the backup data centre and the DR Plan. Without the full implementation of Phase 3, the DR specialists have indicated that, in the event of a disaster, it will take months to complete a full recovery of the City’s critical business applications. In addition, very detailed business continuity plans would have to be developed and sustained by all departments.

As part of the Information Services restructuring, one (1) full-time Information Services staff member will be assigned to manage the data centre, ensure DR plans are kept up-to-date as applications change and execute DR plan tests.
These recommendations have been reviewed with the IS Strategic Team and the IS Working Committee.

**BACKGROUND:**

The City of Hamilton currently relies on a single data centre to run or provide secure Internet access to the majority of applications for all City departments. The applications include Hansen, Avantis, LIMS and Trapeze for Public Works, CLASS and SDMT for Community Services, AVL and FDM for Emergency Services, ISCIS and IPHIS for Public Health, Vailtech, Peoplesoft Finance and HR for Corporate Services, e-mail and the City’s phone systems. The existing data centre houses the infrastructure required for the City’s critical applications and includes approximately one hundred and eighty (180) servers and core network hardware.

Information Services ensures that critical systems can be recovered by performing regular system backups, maintaining documentation on recovery procedures and storing backup media at an off-site location. In the event of a system failure or data loss, the backup media is used to restore a system to its’ normal functioning state. In addition, various levels of redundancy are built into the network infrastructure and servers. Redundant capabilities allow an application to continue running by using readily available backup equipment.

Despite all of these operational activities, the City’s data centre represents a single point of failure. A disaster that affected the data centre, such as a water leak, cooling system failure or fire, would cripple all of the City’s business applications and technology systems.

Ensuring that the City’s critical computer systems can be recovered in the event of a data centre disaster requires a comprehensive IS Disaster Recovery Plan, comprised of several components:

1. **Business Impact Assessment**
   An understanding of priority and recovery time for each of the City’s applications;

2. **Risk Assessment**
   An understanding of the risks to which the City’s applications are exposed;

3. **Backup Data Centre**
   An available location with the computer and network hardware required to recover the systems;

4. **Detailed Disaster Recovery Plan**
   A detailed plan for recovering the City’s applications and systems, including the essential IS employees, required to complete the recovery;

5. **Business Continuity Plans**
   A detailed plan prepared and maintained by each department, including essential employees and detailed plans for operating critical services manually without supporting computer business applications;

6. **Disaster Recovery Plan Maintenance**
   Regular testing and updating of the Disaster Recovery Plan.
1. Business Impact Assessment
The development of a comprehensive IS Disaster Recovery Plan requires a significant amount of effort to assimilate, analyze and draw conclusions regarding the use and dependency of computer applications across the organization. DR specialists were engaged in the project to assist in completing the required investigation and analysis work and to ultimately prepare recommendations to ensure the delivery of a disaster recovery program that would best meet the City’s needs.

Representatives from all City Departments and the Hamilton Public Library participated in the assessment to determine the impact on the City of a disaster which rendered the primary data centre unusable.

Three (3) key dimensions of impact were measured:
- Type of Impact
- Severity of Impact
- Timeframe or Duration of Outage

The following types of impacts were assessed:
- Customer Service
- Business Operations
- Loss of Gross Revenue
- Loss of Public Image/Trust
- Governance
- Loss of Content/Source Data
- Regulatory Compliance
- Extra Expenses
- Employee Health and Safety; and
- Public Safety Issues

The Business Impact Assessment provided compelling information to show that the loss of the data centre would have a profound impact on City staff, citizens and the City’s business. The report, developed by the DR specialists, revealed potential impacts on public safety, inability to meet regulatory compliance requirements, customer service and public image within the first three (3) days of a data centre outage. The report also concluded the financial impact to the City could exceed $3.4M, within the first three (3) days, if the data centre was out of service.

The Business Impact Assessment identified which computer applications were critical to the City and the time period in which they must be restored to operation. The findings revealed that, in order to mitigate risk to the City, a large number of these applications must be available within a four (4) to twenty-four (24) hour period. Over half of the equipment in the data centre would need to be in place in order to meet these timelines.

2. Risk Assessment
A risk assessment was carried out to assess the types of threats that could impact the operation of the City’s data centre. Measurement of frequency and severity was used to determine the threats that were of highest risk to the City.
A number of activities are currently being undertaken to lower the risk associated with identified threats to the current data centre. These activities will help to ensure a more reliable data centre operation but do not eliminate the need for a full IS Disaster Recovery Plan.

### 3. Backup Data Centre
A detailed Disaster Recovery Plan cannot guarantee a quick restore without redundant computer systems and network hardware at a backup location. Since the City does not currently have a backup data centre site, the City’s business applications would be unavailable for weeks or months in the event of a major data centre disaster. Therefore, the disaster recovery planning project explored options for establishing a pre-built backup data centre site. This facility would act as a backup to the existing primary data centre and would enable the City to recover critical business applications in a timely manner.

It is recommended that a backup site be implemented at a City-owned location with the computer and network hardware required for fast recovery. Based on a review of options, it is recommended that the backup data centre be implemented at the new Hamilton Public Library facility in Waterdown.

### 4. Disaster Recovery Plan
Detailed disaster recovery procedures are required to ensure that the required systems can be quickly and efficiently restored to normal operation. Based on the configuration of the backup data centre and equipment, the existing Phase I Initial DR Plan will be updated to include all of the applications identified in the Business Impact Assessment.

Implementing a pre-built backup data centre, together with a detailed Disaster Recovery Plan, will minimize:
- the disruption to City business in the event of a data centre disaster;
- the need for detailed business continuity plans for each of the City’s business units.

### 5. Business Continuity Plans
Detailed plans are required for each City department or business unit to ensure that their critical business processes will continue to function manually in the event of a data centre disaster. These plans must be developed by staff familiar with the department’s business processes. Manual execution of these business continuity plans will require a significant effort on the part of trained staff.

The need for detailed departmental business continuity plans can be minimized if the Information Services DR plan ensures a quick return to normal operations.

### 6. Disaster Recovery Plan Maintenance
A Disaster Recovery Plan must be kept up-to-date. As new technologies are implemented or existing business applications are upgraded, the plan must be updated to ensure that it remains valid and useable in the event of a disaster.
As with the City of Hamilton’s Emergency Operations Plan, a Disaster Recovery Plan must be regularly tested. Tests expose inappropriate assumptions and weaknesses in the Disaster Recovery Plan and continually ensure that critical systems can be quickly restored. Best practices recommend testing IS DR plans annually.

As part of the Information Services restructuring, one (1) full-time Information Services staff member will be assigned to manage the data centre, ensure DR plans are kept up-to-date as applications change and execute DR plan tests. Operating costs for the backup data centre are estimated at $80,000 per year. These costs will be recovered through the capital projects for the first three (3) years, at which time, it is expected that the IS operating budget will reflect and have developed the capacity to absorb the operating impact.

**ANALYSIS/RATIONALE:**

**Requirement for a Backup Data Centre**

The Business Impact Assessment, conducted by the DR specialists, identified that the City would be impacted financially and the City’s ability to deliver services to the public would be affected within twenty-four (24) hours of a data centre disaster. In order to meet recovery time requirements for critical business applications, a backup data centre site must be available.

Without a backup data centre, Information Services staff would have to locate an alternate data centre, prepare the site with proper air conditioning, electrical supply, network cabling, security and order and install computer equipment. All of this would have to be completed prior to recovering any computer applications or data. At best, this work would take four (4) to six (6) weeks to complete which would leave City staff without phones, e-mail and computer applications for that length of time.

The absence of a backup data centre site makes it extremely difficult to test, validate and maintain the existing initial DR plan. Tests of this DR Plan involve only a verbal discussion of steps with no ability to carry out or test any of the recovery procedures.

Without a backup data centre, City departments require very detailed business continuity plans to ensure that their critical business processes will continue to function manually in the event of a data centre disaster.

**Disaster Recovery Backup Data Centre Strategy**

There are four (4) options for implementing a backup data centre:

- **Option A – Status Quo**
  - continue with the single data centre and no disaster recovery capability.

- **Option B - An “in-house” solution**
  - implemented at a City-owned site and operated by City staff.

- **Option C - A “hosted” solution**
  - delivered and managed by an external service provider.
Option D - A Reciprocal Agreement
- involving the sharing of one (1) or more locations between similar organizations with each managing its’ respective environment.

The DR specialists compared each option. Their analysis showed that the “in-house” and “hosted” solutions show no significant differences in initial costs (first five (5) years). Beyond five (5) years, the on-going costs of the “hosted” solution would exceed that of an “in-house” solution. The “in-house” option, however, does offer greater flexibility in sharing production application loads, in data backup processes and in DR plan testing. A Reciprocal Agreement has many disadvantages, including limited reliability, flexibility, security and control by the City. It is, therefore, rarely implemented and not recommended.

The following Chart compares different aspects of the three (3) options that involve a backup data centre:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Option B In-House</th>
<th>Option C Hosted</th>
<th>Option D Reciprocal Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed of recovery</td>
<td>Within Recovery Time Objective</td>
<td>Within Recovery Time Objective</td>
<td>Dependent on agreements and technical specifics</td>
</tr>
<tr>
<td>Reliability of solution</td>
<td>Very reliable</td>
<td>Very reliable</td>
<td>Not reliable – difficult to control / manage</td>
</tr>
<tr>
<td>Security of site</td>
<td>Secure</td>
<td>Very secure</td>
<td>Not secure – multi-organizational access difficult to control</td>
</tr>
<tr>
<td>Flexibility for change</td>
<td>Very flexible</td>
<td>Relatively flexible</td>
<td>Not very flexible, as two entities needs must be considered simultaneously</td>
</tr>
<tr>
<td>Testability of solution</td>
<td>Very testable</td>
<td>Testable</td>
<td>Partial / minimal testing possible</td>
</tr>
<tr>
<td>Control of environment</td>
<td>Full control</td>
<td>Moderate control</td>
<td>Moderate control</td>
</tr>
</tbody>
</table>

The DR specialists recommended an “in-house” data centre site strategy for a number of reasons:
- It provides rapid recovery that meets the recovery time objective of the City’s critical business applications;
- It provides a secure, reliable solution that is under the City’s full control and is always available;
- It provides easy and immediate access to enforce and deploy production changes to the backup environment;
- It provides the ability to test DR plans as frequently as needed;
- It requires lower on-going operating costs than a “hosted” solution;
• It allows the City to leverage and deploy existing resources including servers and the phone system;
• It allows the City to leverage the backup site for creating and storing off-site backups thereby reducing or eliminating the City’s need to use a service provider;
• It allows the City to use the server hardware located at the backup site for application development and testing, freeing up server resources at the primary site.

Information Services staff identified the following additional advantages to the “in-house” option:
• It minimizes the need for each department to have detailed Business Continuity plans. Detailed Business Continuity plans require a significant effort from departmental staff familiar with the department’s business processes. Execution of the Business Continuity plans require a significant departmental staff effort to implement the manual business processes. With an “in-house” data centre that can provide short recovery times, departmental planning does not require the same level of detail. This provides a more cost-effective approach at the enterprise level.

• It allows Information Services to deal with the space crunch in the existing data centre by moving test and development systems to the backup data centre.

Subsequently, Information Services surveyed other municipalities about their DR plans and backup data centres. Of the twenty-three (23) municipalities who responded, fourteen (14) municipalities have backup data centres, all based on “in-house” solutions.

**Disaster Recovery Backup Site Selection**

The following criteria were used to select the recommended location for the City’s backup data centre:
• Distance from the primary data centre. The backup site should be ten (10) kilometres away to ensure it is not affected by the same disaster situation;
• The backup site should also be on the escarpment or well above the level of Lake Ontario;
• A reliable supply of electrical power, preferably not on the same feed as the primary site;
• Proximity to potential sources of disaster (e.g., airport, industrial sites, chemical storage, fires, etc). The backup site should not be located in an area of elevated risk;
• Fibre connectivity to the City's core network with redundant fibre paths;
• Adequate space for equipment, IS staff and storage;
• Accessibility by IS staff with access for equipment deliveries and adequate parking;
• Proximity to overnight accommodations and food;
• Adequate physical security for the facility; and
Capacity for future expansion and availability of optional space for business continuity.

Four (4) potential sites were considered:
- Hamilton Public Library (HPL) Waterdown Library (new site requiring new construction);
- Glanbrook Municipal Service Centre (existing site requiring internal construction);
- Mountain Transit Centre (existing site requiring internal construction);
- Simulated Fire Rescue Complex (new site requiring new construction).

Based on the site selection criteria, the new HPL Waterdown Library site is recommended.

**ALTERNATIVES FOR CONSIDERATION:**

**Disaster Recovery Backup Data Centre Strategy**

**A. Maintain existing plan with no backup data centre.**
The existing plan is a document that provides a process for staff to recover e-mail, Finance, Payroll and the City’s phone system. Without additional equipment available at a backup site, it would take weeks or possibly months, to restore the applications that the City deems to be critical. The impact to the City and City services, without access to these critical applications for that length of time, would be severe. Thorough testing of the existing plan is not possible.

*This option is not recommended.*

**B. Implement a full disaster recovery plan using an “in-house” backup data centre site.**
An “in-house” backup site would involve higher capital costs than a “hosted” site but would result in lower annual operational costs. Control, flexibility and testing would be better than with a “hosted” solution. The “in-house” site could also be leveraged to run test and development servers.

*This option is recommended.*

**C. Implement a full disaster recovery plan using a “hosted” backup data centre site.**
A “hosted” backup site would involve lower capital costs than an “in-house” site but would result in increasing annual operational costs. Control and flexibility of the site would be less than with an “in-house” solution due to strict and sometimes slow change management procedures. Testing of the solution is not as easy due to the complexities of the network and since the “hosted” site would likely be located outside of Hamilton. There is no flexibility to leverage the “hosted” site for any other use.

*This option is not recommended.*
D. Implement a full Disaster Recovery Plan using a shared backup data centre site.
A shared backup site would restrict the City’s ability to maintain and test the site and DR Plan. Control and security of the site would be limited, due to the number of staff from other organizations, who would require access. During a disaster situation, the shared alternate site could be required by any and all organizations at the same time, further limiting the City’s ability to recover quickly. This option would also be slower to deploy since a suitable partner organization would need to be found, costs negotiated and legal agreements established. This option is not recommended.

**FINANCIAL/STAFFING/LEGAL IMPLICATIONS:**

**Financial Implications:**
The total project cost is forecast at approximately $2.0 million, inclusive of the capital cost, as well as three (3) years operating costs, which will allow staff to absorb the operating costs or phase-in any amount needed over three (3) years.

**Staffing Implications:**
Information Services staff will be required to plan, implement, operate and test the backup data centre. Best practices recommend testing the Disaster Recovery Plan at least once per year. Testing will highlight deficiencies in the Disaster Recovery Plan which must then be corrected.

One (1) full-time Information Services staff person will be assigned to manage the backup data centre, maintain an up-to-date Disaster Recovery Plan and complete the required testing on an annual basis.

**Legal Implications:**
There are no immediate legal implications to the selection of a backup data centre strategy or backup site. However, there would likely be many legal implications if the City were faced with a data centre disaster in the absence of an up-to-date and test Disaster Recovery Plan.

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

**RELEVANT CONSULTATION:**
Staff from all City Departments and the Hamilton Public Library participated in the Business Impact Assessment. Staff from the Hamilton Public Library, City Facilities, Hamilton Public Library Security, Risk Management Services and Emergency Management took part in the Risk Assessment.
The City’s Information Services Strategic Committee (ISSC) and Information Services Working Committee (ISWC) provided input and support the recommendations.

**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.

- Community Well-Being is enhanced.  ☑ Yes  ☐ No
- Environmental Well-Being is enhanced.  ☑ Yes  ☐ No
- Economic Well-Being is enhanced.  ☑ Yes  ☐ No

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

The City’s IT network and systems support all of the City’s business applications required for the delivery of all City services to the community.

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

Reliable, resilient IT network and systems provide the environment required for City staff to deliver services to the public.