

# Technology Disaster Recovery Planning

The original recommended practice was developed by the Government Finance Officers Association (GFOA). Some aspects of the practice have been revised by the Financial Management Capacity Building Committee (FMCBC) for use by Nova Scotia municipal governments. The original GFOA recommended practice is *Computer Disaster Recovery Planning*, approved by the Committee on Canadian Issues in June 2000, but was revised as the *Technology Disaster Recovery Planning* recommended practice in 2007. Other sources used are footnoted in the text.

## Recommendation

The GFOA recommends that every government formally establish and regularly update written policies and procedures for minimizing disruptions resulting from failures in computers or other advanced technologies following a disaster. The FMCBC agrees with this recommendation.

## Purpose

Disruptions in a municipality's provision of essential services are likely to cause significant harm or inconvenience to those whom a municipality serves. A formal plan for technology disaster recovery (TDR) helps municipalities to fulfil their service obligations to citizens by minimizing interruptions following a disaster. (See *Appendix I* for a more extensive discussion on benefits and costs.)

## Background

Today, the public sector, like the private sector, relies heavily upon computers and other advanced technologies to conduct its operations. Therefore, emergency measures planning, to be effective, must specifically address policies and procedures for minimizing the disruption of municipal operations if computers or other advanced technologies are disabled following a disaster.

A TDR plan can be referred to as an emergency measures plan. An emergency measures plan is, following the definition stated in the *Emergency Measures Act* (EMA), a plan, program, or procedure prepared by a municipality (or the province) that is intended to mitigate the effects of an emergency or disaster and to provide for the safety, health, or

welfare of the civil population and the protection of property in the event of such an occurrence.<sup>1</sup>

For the purpose of this practice, a disaster refers to a non-planned event that significantly interrupts the function of a municipality's computer system or other advanced technology. Examples of disasters are power outages, fire, explosions, gas or other toxic-substance accidents, damage to telecommunication lines, computer viruses or worms, hard disk crashes, memory failures, and natural disasters (flooding, hurricane etc.). The access to a TDR plan is essential after both a community-wide disaster (e.g. natural disaster, power outage) and an isolated disaster (e.g. institutional fire, computer virus). Even if a disaster does not directly damage computers or other advanced technology, it can still limit the access to such equipment and thereby interrupt the municipality's operations (e.g. during a gas leak close to the town office).

It is important to realize that TDR planning is not just an information system issue. Information system staff can deal with technical issues, but management needs to address central questions such as organizational priorities, backlogs, and the degree of dysfunction that can be tolerated.<sup>2</sup>

## Considerations in Policy Development

At a minimum, a municipality should do the following when developing policies and procedures for a formal TDR plan (a more extensive discussion of each element can be found in *Appendix I*):

- 1) Consider total *costs and benefits*
- 2) Assign disaster recovery *coordinators*
- 3) Require the *creation and preservation of back-up data*
- 4) Enable *alternative processing* of data (extracts from the EMA can be found in Appendix II)
- 5) Provide detailed instructions for *restoring data files*
- 6) Establish *guidelines* for the *immediate aftermath* of a disaster
- 7) Establish a plan for *periodic tests, reviews, and updates*
- 8) Review the TDR plan's *relationship to other emergency measures programs*
- 9) Review the adequacy of TDR for *outsourced services*
- 10) Consider an *expansion* of emergency preparedness

## Appendices

Appendix I: Consideration in Policy Development

Appendix II: Extracts from the *Emergency Measures Act*

## Appendix I: Considerations in Policy Development

### 1) Consider Total Costs and Benefits

The determination of the ultimate strategy for TDR should be based on the risks, their impact, and cost/benefit to the municipality.<sup>3</sup> The costs of developing a TDR plan is low in comparison with the benefits gained when a disaster occur even if the probability for a disaster is very small.

A TDR plan reduces the financial risk for the municipality. For example, a loss of all of a municipality's tax receivables information could result in a significant financial loss. It is important to identify the most critical functions and prioritize the security of these data files. Financial losses also include loss of information and staff time allocated to recreate the data by manual means.<sup>4</sup> Indirect costs for not having a functioning TDR plan when a disaster occurs are, for example, overtime, fines (for not fulfilling legal obligations), punitive payments (e.g. late payment of supplier invoices incurring interest charges), and opportunity costs.<sup>5</sup>

Finally, a TDR plan also reduces the risk of making incorrect or inappropriate decisions in a stressful situation, since the policies and procedures that should be followed are already stated.<sup>6</sup>

One way of reducing the costs following a disaster is to ensure that the municipality has insurance that includes data-processing coverage.

There are several factors that affect the total cost of developing and maintaining a TDR plan, and more expensive alternatives are not necessarily the most effective strategy.

### 2) Assign Disaster Recovery Coordinators

Disaster recovery coordinators should be assigned for each agency or department to form a disaster recovery team (the team can include both managers and technical staff). The following elements should be recorded in the TDR plan related to the disaster recovery team:

- A current list of the team members;
- Phone numbers for all team members (updated periodically);
- Plans for alternative ways of communicating (e.g., cellular phones); and
- Procedures for assembling the team in the event of a disaster.

It is important to make the TDR plan visible for other staff members, outside the team. The incorporation of the TDR plan in an education and awareness program can ensure that all system owners are aware of the plan.

### **3) Require the Creation and Preservation of Backup Data**

Properly creating and preserving backup data are key elements in a TDR plan. A municipality's procedures in this regard should cover the regular and timely backup of computer data and the transportation and storage of backup data off site. Backup data should be created on a daily basis in order to minimize the risk of information loss. It is recommended that the data and a copy of the TDR plan are stored off site at a location that will not be affected by a potential disaster (8 km away if possible<sup>7</sup>). The municipality should also ensure the security of backup data both during transport off site and during storage off site, in terms of fireproofing, protection against theft, etc. Security requirements for data files with different sensitivity classification (none, low, medium, or high) and access requirements to these files should be incorporated in the TDR plan.

This includes special storage (e.g. in a vault, fireproof storage etc.) and access requirements based on the classification and privacy levels of the data.

There are several methods that can be used for creating backup data including backing up a network drive, local tape backup devices, and use of software that handles the backup automatically.<sup>8</sup>

Determination of the most appropriate method for backing up data should consider the advantages in security and accuracy of different backup methods. Manual backups conducted by individual users can, for example, be the cheapest alternative, but experience shows that such a system does not create proper backups.<sup>9</sup>

### **4) Enable Alternative Processing of Data**

Municipalities should make provision for the alternative processing of data following a disaster. Methods for alternative processing of data are key components in business continuity planning. Business continuity planning refers to the process of identifying critical operational systems and ensuring the continuing availability of those systems after a disaster. Some procedures can be conducted manually while others require the use of supplementary, technical equipment.

The EMA allows municipalities to enter into agreements with other municipalities, persons, or an organization for the purpose of emergency measures plans (see Appendix II). It is important that a mutual aid agreement or a contract has a formal character and that it ensures that compatible computers and other technical equipment are available on short notice.<sup>10</sup> A municipality should ensure that the alternative processing site remains capable of processing the municipality's data.

There are at least three main issues in the context of alternative information processing that need to be addressed by management, in consultation with affected staff:

- How will employees conduct their work when the system is down? <sup>11</sup>
- What is to be done with the processing backlog that has built up during the interruption? <sup>12</sup>
- What priorities for data processing should apply if the use of the alternative processing site becomes necessary?

### **5) Provide Detailed Instructions for Restoring Data Files**

The TDR plan should include detailed instructions for restoring data files. The degree of detail should be on a level that makes it possible for non-technical staff to conduct the basic procedures.

Management needs to address the following issues while constructing policies on restoring data files and recovery of computer systems:

- How fast is recovery needed? <sup>13</sup>
- Which systems must be recovered first? <sup>14</sup>

The answers to these questions should be answered based on the municipality's own priorities and cost/benefit analysis, as earlier stated in *Section 1*.

### **6) Establish Guidelines for the Immediate Aftermath of a Disaster**

It is important that municipalities establish guidelines for the immediate aftermath of a disaster. It is essential to keep citizens and stakeholders informed on the effects of the disaster and progress of the recovery process. <sup>15</sup> The municipality's TDR plan should provide guidelines for the following:

- Notification that an event has occurred;
- Issuing of press releases;
- Legal issues;
- Contacts with the media;
- Procedures for recovering communications networks; and
- Procedures for assessing damage.

### **7) Establish a Plan for Periodic Tests, Reviews, and Updates**

It is absolutely necessary that a municipality regularly test, review, and update its TDR plan. Tests, reviews, and updates should be conducted on a periodic basis and when carrying through significant system changes (e.g. organizational changes, software and hardware updates). <sup>16</sup> There are a number of problematic dysfunctions that can be discovered while conducting a test.

- Failure to utilize a mutual aid agreement or other agreement with a third party (e.g. incompatible equipment);
- Lack of preparation in terms of staff training; <sup>17</sup>

- Lack of resources (material or staff) for applying the TDR plan;<sup>18</sup>
- Exceeding the target time for the recovery process;
- Lack of coherence in the TDR plan as a whole; and
- Technical problems with backup data and restoring procedures.

The following considerations should be made while testing a TDR plan:<sup>19</sup>

- *Full-scale tests versus isolated tests.* There may be an advantage in testing components in isolation, since a full test might result in extensive disruptions. Isolation also allow for quicker localization of problems that might occur during the test. A final review of the functioning of all components, as a whole, should then be carried out to ensure that everything fits together.
- *Realistic approach.* People involved will improve their ability to respond correctly when a real disaster occurs if the test is based on a realistic scenario. A staff member should act as an observer during the test to ensure that involved personnel have not taken short cuts.
- *Third party reliance.* Agreements on mutual aid and procedures that in other ways involve a third party should be practically tested if possible (see *Section 3* for a discussion on mutual aid).

Individuals that participate in the test should also take a part in the review afterwards. The review of the test provides the base for an update of the TDR plan. A review and update should also be carried through when a disaster has occurred. At least the following aspects should be evaluated in the operational review:<sup>20</sup>

- Causes of the incident;
- Adherence to plans and procedures by the organization;
- Validity of plans and procedures;
- Adequacy of training; and
- Availability of appropriate resources.

## **8) Review the TDR Plan's Relationship to Other Emergency Measures Programs**

The EMA requires that all municipalities have an emergency measures organization, an emergency bylaw, an emergency plan, an emergency measures coordinator, and a standing committee of council (see Appendix II).<sup>21</sup> How the TDR plan relates to the mandatory and optional elements will vary among municipalities. It is up to each municipality to review all components and ensure overall consistency.

## **9) Review the Adequacy of TDR for Outsourced Services**

A municipality also should satisfy itself concerning the adequacy of emergency plans for outsourced services, including TDR plans. It is possible to integrate minimum

requirements on emergency plans in a contract with a service provider. A system for feedback or oversight audit should also be established to ensure that the service provider fulfils the requirements.

#### **10) Consider an Expansion of Emergency Preparedness**

Emergency preparedness is a continuous cycle of planning, testing, training, and evaluation.<sup>22</sup> The TDR plan is just one of many possible emergency measures plans. The Provincial Emergency Measures Organization has developed a tool to assess municipalities' emergency preparedness, which can be found on their website (see the reference list for the web address). Section II of the *Nova Scotia Emergency Management Manual* provides an overview of municipal emergency planning including planning stages, risk-assessment tools, a plan development guide, operations centre considerations, emergency simulation exercises, an overview of emergency site management, and guidelines for developing mutual aid agreements.<sup>23</sup>

## **Appendix II: Extracts from the Emergency Measures Act**

### **Duties of municipalities**

**10 (1)** Within one year after the coming into force of this Act, each municipality shall

- (a) subject to the approval of the Minister, establish and maintain a municipal emergency by-law;
- (b) establish and maintain a municipal emergency measures organization;
- (c) appoint a coordinator of the municipal emergency measures organization and prescribe the duties of the coordinator which shall include the preparation and co-ordination of emergency measures plans for the municipality;
- (d) appoint a committee consisting of members of the municipal council to advise it on the development of emergency measures plans; and
- (e) prepare and approve emergency measures plans.

### **Powers of municipalities**

**(2)** The municipality may

- (a) pay the reasonable expenses of members of the organization or members of the committee appointed pursuant to clause (b) or (d) of subsection (1);
- (b) enter into agreements with and make payments to persons and organizations for the provision of services in the development and implementation of emergency measures plans;
- (c) enter into an arrangement or agreement with any other municipality respecting a common organization, plan or program;
- (d) appropriate and expend sums approved by it for the purpose of this Section. 1990, c. 8, s. 10.

## References

- Baker, Gary. "Quick Recoveries". CA Magazine. 128, no 6 (1995): 49-51.
- Cerullo, Michael J.; Steve R. McDuffie and Murphy L. Smith. "Planning for Disaster". The CPA Journal. vol. 64, issue 6 (1994): 34-38.
- Emergency Management Office, Province of Nova Scotia. Tools for Emergency Management Practitioners.  
<http://www.gov.ns.ca/emo/AbsPage.aspx?ID=1175&siteid=1&lang=1>.
- Government Finance Officers Association. Technology Disaster Recovery Planning, Approved June 2007.  
<http://www.gfoa.org/downloads/caafotechnologydisaster.pdf>.
- Hawkins, Henry. "Are You in the Dark About Disaster Preparedness?". Kentucky Banker Magazine. no 849 (May 1997): 18-21.
- Hickman, Thomas. "How to Stay Connected". Strategic Finance. 84, no 3 (2002): 32-35.  
International Federation of Accountants. Small and Medium Practices Task Force. December (2003).
- Laidlaw, Robin, Roger Marshall, Richard Woods, John Butters and Sharm Manwani. "How Can You Test Disaster Recovery Plans?". Computer Weekly. Jun 15, 2004: 26.
- Nova Scotia. Emergency Measures Act of Nova Scotia. R.S.N.S. 1990, Chapter 8.
- "The Right Question for a New Disaster". The Practical Accountant. 35, no 1 (2002): 10.
- Ulfelder, Steve. "Classic Mistakes". Computerworld. 38, no 16 (2004): 36.

## Notes

- <sup>1</sup> Nova Scotia. *Emergency Measures Act of Nova Scotia*. R.S.N.S. 1990, Chapter 8. Section 2 (d).
- <sup>2</sup> Compare to Baker, Gary. "Quick Recoveries," *CA Magazine* 128, no 6 (1995): 49-51. And to Ulfelder, Steve. "Classic Mistakes," *Computerworld* 38, no 16 (2004): 36.
- <sup>3</sup> Baker, Gary, 1995.
- <sup>4</sup> Compare to Hawkins, Henry. "Are you in the dark about disaster preparedness?," *Kentucky Banker Magazine*, no 849 (May 1997): 18-21.
- <sup>5</sup> International Federation of Accountants. Small and Medium Practices Task Force. *Controlling Computers in Business: Computer Disaster Recovery Planning*. The fifth in a series of guidance documents for SMPs and SMEs. December (2003).
- <sup>6</sup> International Federation of Accountants, 2003.
- <sup>7</sup> Hawkins, Henry, 1997.
- <sup>8</sup> Hickman, Thomas. "How to stay connected", *Strategic Finance*, vol. 84, issue 3 (2002): 32-35.
- <sup>9</sup> Hickman, Thomas, 2002.
- <sup>10</sup> Compare to Cerullo, Michael J., Steve R. McDuffie and Murphy L. Smith. "Planning for Disaster," *The CPA Journal* 64, no 6 (1994): 34-38.
- <sup>11</sup> Baker, Gary, 1995.
- <sup>12</sup> Baker, Gary, 1995.
- <sup>13</sup> Baker, Gary, 1995.
- <sup>14</sup> Baker, Gary, 1995.
- <sup>15</sup> Compare to "The Right Question for a New Disaster," *The Practical Accountant* 35, no 1 (2002): 10.
- <sup>16</sup> Compare to Laidlaw, Robin, Roger Marshall, Richard Woods, John Butters and Sharm Manwani. "How can you test disaster recovery plans?," *Computer Weekly*. Jun 15, 2004: 26.
- <sup>17</sup> Compare to Emergency Measures Organization, Government of Nova Scotia. *Evaluating Municipal Emergency Preparedness*.
- <sup>18</sup> Compare to Emergency Measures Organization, Government of Nova Scotia. *Evaluating Municipal Emergency Preparedness*.
- <sup>19</sup> Compare to Laidlaw, Robin, Roger Marshall, Richard Woods, John Butters and Sharm Manwani, 2004.
- <sup>20</sup> Compare to Compare to Emergency Measures Organization, Government of Nova Scotia. *Evaluating Municipal Emergency Preparedness*.
- <sup>21</sup> Government of Nova Scotia. *Emergency Measures Act of Nova Scotia*. Section 10 (2), (1990).
- <sup>22</sup> Compare to Emergency Measures Organization, Government of Nova Scotia. *Evaluating Municipal Emergency Preparedness*.
- <sup>23</sup> Emergency Measures Organization, Government of Nova Scotia. *Nova Scotia Emergency Management Manual*.