Mid-size Canadian Businesses Investment in BCM

How to proactively prevent disruptions and react to interruption of vital operations

Karim Najjar, Dr. Shaun Aghili, Prof. Ron Ruhl
Information Systems Security Management Concordia University College of Alberta, Canada
knajjar@student.concordia.ab.ca, {shaun.aghili, ron.ruhl}@concordia.ab.ca

Introduction

Abstract

The term disaster recovery is not widely used in mid-size businesses as of a study done by Lock, T., Bennett, B., & Vile, D. (2011) [1]; though it is a major consideration when examining information security procedures put in place. Disaster Recovery directly impacts the three principles of security; namely, Confidentiality, Integrity and Availability (CIA). In other words, an effective, fully implemented and regularly tested disaster recovery plan is a necessary risk management component for all enterprises. . The implementation of any Business Continuity Plan / Disaster Recovery Plan (BCP/DRP) plan includes managing people, data, infrastructure, resources and critical operations at the time of an incident that might escalate to a disaster.

Failure in designing and implementing an effective BCP/DRP plan for a medium size businesses will result in catastrophic size financial losses for such enterprises and thus a significant threat to their post-disaster sustainability. According to Widup (2003) twenty six point one percent (26.1%) of the companies that have disaster recovery plans never had those tested [2]. The latter also notes that disasters are not exclusive for both natural and terrorism causes, but also human errors and failures.

When studying Information Security; Disaster Recovery acts as both the bed rock and umbrella that assures all three aspects of security "CIA" (Confidentiality, Integrity and Availability) are maintained and before considering any security controls, latest technologies, policies or technical based solutions; an enterprise should have a well-established disaster recovery plan to mitigate the risk of going out of business. The proposed framework will take into account constraints such as geographic location, regulations and limited budget. The term "Midsize", as used in the context of this research project is based on the categorization used by *Statistics Canada* [3], (http://www.statcan.gc.ca) that considers any enterprise with an annual operating revenue between 25 million inclusive and up to 75 million dollar. According to a report prepared by *Industry Canada* [4] (http://www.ic.gc.ca), the number of midsize Canadian businesses operating in Canada exceeds eighteen thousands in 2012. *Industry Canada* also mentions that medium sized Canadian enterprises have a range of 100 and 499 full-time employees. The budget of the proposed framework would be up to three percent (3%) from the overall yearly gross revenues. According to [5], [WU1]companies with revenues less than $250 million are spending two percent (2%) of yearly revenues on DRP plans. Also, according to a survey done by *Disaster Recovery Journal* (http://www.drj.com/) [6], fifty three percent (53%) of respondents on the survey spent less than ($500,000) annually on DRP in 2007 but according to Forrester's Global IT Budgets , Priorities, And Emerging Technology Tracking Survey; Q2 2010, thirty six percent (36%) of SMEs plan to increase spending on BC/DR by at least five percent (5%) [6] . Though there are different approaches and researches done on how to calculate cost of downtime and then plan accordingly, this research considered three percent (3%) of yearly gross revenues as a maximum amount to budget an effective and efficient DRP/BCP framework.

Mid-size businesses must have a business continuity plan in order to face challenging situations. There are no exact figures on how much an hour of downtime might cost an enterprise, but it is not hard to imagine that for some- if not most- the financial consequences of only a few hours of down time can be substantial. Enterprises will always try to avoid declaring a disaster because executing a disaster recovery plan is complex, risky, and expensive [5]. Business Impact Analysis (BIA) will define at what point a recovery plan should be triggered and to what extent can an enterprise handle consequences of a disaster. Testing of those plans is a challenging task, if not planned or managed well, but the risk associated with not having those plans in action exposes the enterprise to the threat of going out of business. According to Kavur (2009), each downtime incident cost a Canadian Enterprise a medium of $ 496,500 US [7].

Problem Statement

According to the Gartner Group, two out of five companies that experience a catastrophe, or an extended system outage, never resume operations; of those that do, one-third will go out of business within two years. The Federal Emergency Management Agency (FEMA) states that Forty percent (40%) of businesses do not reopen following a disaster and another twenty five percent (25%) fail within one year [8]. A common belief among medium size businesses' high level management executives is that disaster recovery and business continuity plans are very costly, and in most cases not needed for smaller operations. The Gartner Group and FEMA studies clearly show that failure to develop and implement a cost effective disaster recovery and business continuity plan can seriously jeopardize an enterprise's operations following a disaster to the point of insolvency. As of a survey conducted by Symantec (2011), fifty two percent (52%) of enterprises without a DRP plan answered that they don't think computer systems are critical to the business while forty one percent (41%) said that it never occurred to them to put together a plan, and forty percent (40%) said that disaster preparedness is not a priority [9].

Table of Acronyms:

The following acronyms will be continuously used in this research

Terms	Abbreviation
BCM	Business Continuity Management
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
IRP	Incident Response Plan
ERP	Emergency Response Plan
BIA	Business Impact Analysis
NIST	National Institute of Standards and Technology
SME	Small Medium Enterprises
DRT	Disaster Recovery Team
ROI	Return on Investment

Table 1 Acronyms Definition

Research Objectives

The research paper will address [WU2] the following objectives:

1. To **propose** an effective and financially feasible Disaster Recovery/Business Continuity (DR/BC) **Framework** that is compatible with Midsize Canadian Businesses.
2. To provide **recommendations** for the **implementation** of a DRP for a midsize Canadian enterprise, based on the proposed framework.
3. To provide a template to be used for **budgeting and control purposes** based on the proposed DR/BC framework.
4. To align (map) the proposed framework to COBIT 5 for Risk

Background

According Kopytoff (2012), [WU3]disaster planning plays an important role in ensuring the resume of operations after a disaster [10]. When drafting any framework, policies are engaged to make sure what is proposed aligns with rules and concerns already there. In addition to that, according to Hamidovic (2011), risk management plays a big role when trying to define what are the organization's assets and resources in order to give them a monetary value to calculate loss in case those resources went down [11].

When considering the risk impact of any incident on the daily operations of mid-size businesses, it is critical to perform a BIA (Business Impact Analysis). According to Johnson (2008), BIA is a tool to figure out what essential business units are needed for survival of the critical operations in addition to the RTO (Recovery Time Objective); period of time allowed for recovery and RPO (Recovery Point Objective); point in time where data must be recovered to resume ordinary operations. In other words, it enables high level managers determine to what extent they can handle risk "Risk Appetite" and at what level any plan has to be triggered [12]. According to (ISACA), Business Impact Analysis is identified based on worst-case scenario that assumes that the physical infrastructure supporting each respective business unit has been destroyed and all records and equipment are not accessible for 30 days" [13].

BCM (Business Continuity Management) is the umbrella which covers all plans of recovering from an incident or a disaster starting with an emergency response plan until the actual recovery plan. According to John (2005), the CISO (Chief Information Security officer) reports meaningful data points to senior management, as well as, establishes the threat level for the entire organization [14]. It is worth mentioning that an incident is the early stage of a disaster and that incident response planning comes at an earlier stage. Under BCM comes BCP which maintains a competitive advantage when trying to expose resources to internal/external threats with an objective of providing a preventive and effective recovery option to the enterprise.

According to Hamidovic (2011), emergency response is the initial response when a disruptive incident takes place. It usually involves the protection of people and property from immediate harm [11]. At the second level, Continuity Response is when the processes, controls and capabilities of any organization are back to operation and can meet the critical objectives of the organization. At a later stage; Recovery, is where resources have to be reestablished to meet ongoing operational requirements. It's good to mention here that disaster recovery is a reactive plan to solve business and system outages. While BCM is preventive, DRP is the final plan that has to be triggered after a disaster takes place.

A common belief among medium size businesses' high level management is that disaster recovery and business continuity plans are very costly, and in most cases not needed for smaller operations. Symantec, (2011) published a survey concluding that forty seven percent (47%) of midsize companies with between 100 and 1,000 number employees didn't have a recovery process in place [9]. Also, despite warnings, most SMEs are still not prepared for disasters [9]. It is worth mentioning here that management executives and business owners of medium size businesses said that they consider disaster preparedness whenever they try to decide upon implementing a new technology like private clouds, public clouds and virtualization, (Symantec, 2012) [15].

The survey done by Symantec (2011), also found that sixty five percent (65%) of SMEs are located in regions that are considered susceptible to natural disasters [9]. The survey was conducted on a 1288 SME sample. The second finding was that in 2010, a median of six outages took place mainly resulting from employee errors, cyber-attacks, power outages and wrong updates. The last important part of the survey was that SME's mostly react when it is too late. In other words, they react but do not prevent and only when a disaster occur, do they consider having a plan.

Furthermore, business owners and accounting executives always look at ROI whenever they approve a certain plan. The case is different when it comes to BCM/DRP since there is no clear way to calculate what the return on investment would be if we implement those plans. It is more likely that those plans have to be considered strategic decisions since they deal with the availability and continuity of the business itself rather than discussing how the business can make money by implementing those plans to their business.

Calculating the cost of downtime varies from one business to another since the calculation can be based on peak working times, number of transactions per day, number of employees, cost to recover a single document and other related details. According to Symantec, (2011), the median cost of down time for a medium size business is around $23000 per day which sheds the light on quick solutions that some IT professionals consider to avoid that cost [9]. One of those solutions that have been increasingly emerging is the cloud services. Cisco predicts that more than fifty percent (50%) of all data center workloads will be processed in the cloud [16].Registering to a cloud or being hooked up to cloud services is considered to be an effective way to both prevent and be prepared for any incident that might escalate to a disaster according to IT professional. In fact, a very important issue here is that cloud services are considered as a two edged sword. They do help in safely backing up information but they too have their counter backs. People forgot the idea that a cloud service is a physical service somewhere else. In other words, when a business has an account on a cloud service, it is actually accessing a physical service stored somewhere through the cloud. Not only that, according to Kovar (2012); in his online report *8 Surprising Disaster Recovery Stats*, the most common cause was unexpected update and patches while the following cause was human error in general [17]. To emphasize on that, disasters are not only those big natural events that strike a whole city and destroys everything. Human error and misconfiguration are the most common incidents that result in disasters which indicates that even cloud services are not exempted from disasters.

Quality Technology Solutions (QTS) has a template entitled *10 Steps to Implement a Disaster Recovery Plan*. QTS is an American based organization that provides IT solutions; their template reviews the strategies for implementing a DRP. The firm emphasizes on the point that a BCM is more about identifying the threats that can impact the organization in addition to the mitigation strategies, while DRP is about reacting to the disaster rather than preventing it from happening [18].

The ten steps that they discuss start with 1) Define [WU4]key assets, threats and scenarios. 2) Determine the recovery window 3) Define recovery solutions 4) Draft the DRP Plan 5) Establish communication plan and assign roles 6) Disaster recovery site planning 7) Accessing data and applications 8) Document the plan in details 9) Test the plan and lastly Refine and Retest the plan..

Another BCM template "*DMU template*" that has been prepared by Sanders (2004) is divided into four main broad sections that can be customized to include all threats and mitigation strategies [19]. The first section is the introduction where the template identifies the different meanings of interruptions, disasters, and emergencies. Introduction also includes the objectives, principles, functions, communication and layout guide for the whole document. The template then introduces two different main sections that deal with company contacts in a case of an emergency/ disaster and the other section is the supplier contacts. Those two sections act as a communication plan or tree for the DRT. The last section of the template focuses on the risks, what to do during the incident, after the incident, what is the mitigation solution provided for each risk identified and what constraints the DRT might face.

The third template examined is prepared by (SunGard Availability Service) [20] . The template mentions in the executive overview that regardless of the difference in business the company conducts, or the industry the business falls under, BCM/DRP plans conform to same logical template. The template also identifies the purpose of any BCM/DRP plan as the same for any organization which is documenting specific procedures to be performed before a disaster is declared, during the disaster and after. The introduction section includes the purpose, objective, scope, scenarios and assumptions. The next section identifies the recovery strategies and activities in terms of tasks and personals (DRT Team). Furthermore, a timeline is included in order to help address the RTO and RPO in a timely manner whenever a risk and a mitigation strategy is considered. It also has sections that discuss the disaster declaration process, employee contact information. Vendor contact information and other checklists and forms that have to be prepared whenever a disaster is declared.

The last template that this research examined is prepared by *Admin Service* (www.adminservice.com) [21]. The template is divided into fifteen sections that discuss the importance of having a plan, defines what a DRT is, discusses the evacuation routine and procedures in addition to examining specific disasters such as winter storms, terrorism bombs, and political disasters. The template also mentions the importance of having a communication plan continuously updated and ready for both the DRT and vendors that the business work with.

One of the frameworks discussing contingency planning for federal information systems is NIST 800-34 [22]. It emphasizes on the importance of having a contingency plan ready and continuously tested and guides businesses to draft those plans. NIST breaks down the steps into seven starting with drafting the contingency planning policy statement as a first step, then conducting the BIA, followed by identifying preventive controls, creating contingency strategies, developing the contingency plan, ensuring that planning, testing and training are conducted, and finally making sure that maintenance for those plans are scheduled.

As of a 2013 study done by the Canadian Red Cross; 5,000 small earthquakes are recorded in Canada each year. They strike suddenly and without any previous warning [23]. Floods; in the second place, are [WU5]also costly Canadian disasters. According to Red Cross, 8,000 forest fires in Canada each year and forty five percent (45%) of those fires are caused by lightening; furthermore, the *Atlantic Hurricane Season* lasts from June to November each year in and all it takes is one of these hurricanes to make massive damage. Flu season in Canada runs from November to April each year and an estimated 5 to 10 percent of Canadians get influenza [WU6]each year [23]. Landslides, power outages, thunderstorms, tornadoes and winter storms are on the top Canadian disasters as well. Also, before 1950, Canada has on average of more than one disaster per year, on average of one disaster per year from 1950 until 1998 and then the number drops thereafter [24], *Canadian Disaster Historical Survey*.

Methodology

Business size is usually categorized according to number of full time employees or according to yearly revenues and sometime according to yearly profits. As previously mentioned, since the scope of this research is medium sized Canadian businesses, Statistics Canada's criteria to identify the size of the business will be used. According to the latter, any enterprise that has yearly operating revenue between 25 million inclusive and up to 75 million dollars is considered as medium size [3]. Total number of those businesses currently operating in Canada according to a research conducted by *Industry Canada* (http://www.ic.gc.ca/) is 181, 69 enterprises [4].

As per the discussion earlier in the research; according to Balaouras (2008), spending two percent (2%) of the yearly revenues is a common practice for businesses with less than $ 250 Million yearly revenues [5]. This research will consider deducting three percent (3%) from the minimum yearly revenues and considering it as a budget for the proposed framework. In other words, if the minimum yearly revenue is 25M per year, than three percent (3%) will give us seven hundred and fifty thousand Canadian Dollars ($750,000) to implement, fund, and maintain the framework.

Criteria for choosing suitable available template

The limitation of the current available templates mainly is regarding the location and size of the business. When a business considers implementing a BCM/DRP plan, it has to be tailored to the size of the business since the budget is based on the yearly revenues of the business. Also, the geographic location specifies what threats are common and others that are least likely to happen. As an example, terrorism and explosions are least likely to happen in Canada whereas are considered a high probability if the case we are building is in the Middle East. In other words, the location constraint is more about the threats that are associated with operating in that specific location.

NIST 800-34 is a 7 step contingency planning process that provides guidance and instructions on how to recover information systems after a disruption. The guidance might mention relocation to an alternate site which the research will include in the "Putting Template to a test" section.

NIST document will be used to determine the most relevant available template to be used as a base model for our proposed work [22]. The seven steps that the NIST 800-34 document is divided into are:

1) Develop contingency planning policy statement
2) Conduct the business impact analysis (BIA)
3) Identify preventive controls
4) Create contingency strategies
5) Develop an information system contingency plan
6) Ensure plan testing, training and exercises
7) Ensure plan maintenance

Based on the above steps, the template prepared by Sanders, Glenn (2004) [19] meets all of the above criteria except for the contingency plan policy and conducting the BIA. The research based the proposed framework on Sanders template taking into consideration the best practices discussed in the previously examined three documents [21] [18] [20]. The constraints of size and location were then applied and best practices in the field to have the tailored and customized framework that aligns with strategies of businesses, limited budget, and the location.

Keeping size, location and budget in mind, the research moved to the next level which is keeping track of expenses of the disaster recovery solutions that were provided as best practices. The total amount was less than three quarters of a millions, giving decision makers room to customize the proposed framework based on specific and special needs of each organization.

After drafting the framework was done, the latter was aligned to COBIT 5 for Risk in order to make it possible for any Midsize Canadian organization that is COBIT 5 Risk compliant to implement the proposed DRP framework.
The following is the case that this research has built taking a hypothetical company that operating in Edmonton, Alberta as an example.

Canadian SME Disaster Recovery Framework

Overview

This Disaster Recovery/Business Continuity framework is tailored to "Midsize" Canadian businesses according to a limited budget. The constraints are based on the probability of a threat in a certain location (Canada) and the budget that can be allocated to take action and mitigate the risk (Up to ¾ Million Dollars CDN $ 750,000).

Principles

- ➢ Building risk scenarios and mitigation strategies that are associated with the proposed case.
- ➢ Risks are assessed on the basis of probability and impact.
- ➢ Action and mitigation plans must be reasonable, feasible, practical and achievable.
- ➢ Virtual solutions are key elements of this framework due to cost efficiency.
- ➢ Alternate warm site solutions (privately owned) or agreements with vendors are provided based on availability according to geographic location.
- ➢ Identifying responsibilities, accountability and engaging employees is a key requirement.
  Note: This framework does not cover every possibility. Extreme cases are unpredictable.

Objectives

- ➢ Mitigate the risk associated with any incident that might escalate to a disaster.
- ➢ Restore day to day operations in a timely manner
- ➢ Comply with regulations
- ➢ Continuously test the current plan and make sure it is practical and achievable.
- ➢ Engage top management and decision makers in the process

Sections of Framework

1) The DRP should have a policy that assigns privileges and roles of the DRT when a disaster is declared.
2) Emergency communication plan must be available and continuously updated with active phone numbers and current employees with departments and roles clearly stated.
3) Testing is as crucial as the plan itself when a team is drafting the plan and implementing it since effectiveness of a disaster recovery plan cannot be proved otherwise

Future Changes

This framework is subject to change whenever there is a need to do so. Any of the following might trigger a change request as an attempt to customize the framework to accommodate any emerging trends.

1. New threat being identified as an emerging risk in the geographic area.
2. New technology being available to mitigate risk more efficiently.
3. New service launched that encompasses specific threats when being operated.
4. Change in customer needs.

Precedence

In a case of a conflict, the organization's security policy overrides the Disaster Recovery template.

Disaster Recovery Framework

Disaster Group	Natural Disasters					Human Error			IT/ Technical & Other			
Disaster	Power Outage	Snow Storm	Fire	Floods	Land Slides	Configuration	Short Supply	Construction	Heating Outage	Security	Pandemic	Explosions
Probability	Medium	High	Medium	High	Medium	High	High	Medium	High	High	Medium	Low
Functions Affected	All	All	All	All	All	All	All	All	All	All	All	All
Impact	Medium	High	High	High	High	Medium	Medium	Medium	High	High	High	High

Disasters are divided into three main groups. Under each group, specific incidents or disasters are mentioned with the likelihood or probability of occurrence and the cost to mitigate those disasters.

Please check for full version of the template [WU7] https://docs.google.com/file/d/0BxDnXKXRd3npQ2d6Wm9ab2MwZGM/edit?pli=1

Natural Disasters

Power outages are very common in Canada and are often caused by freezing rain, sleet storms and/ or high winds that usually damage power lines [23]. During summers, government of Alberta often alerts citizens to reduce the use of power because the high demand on the electric grids causing overheating [23]. When a power outage occurs, systems are completely down, day to day tasks cannot be carried. Businesses are also left with no air conditioning whether it is heating or cooling, light, hot water or even sometimes running water.

Snow Storms and floods are considered high probability threats that have to be considered whenever a Canadian business is drafting a disaster recovery framework. The latter is highly common especially when temperatures fluctuate quickly from freezing to warm leading to a very quick massive ice melt and rise in river water levels. Floods are considered to be the most common and costly disasters in Canada [23]. Heavy or steady rain for several hours or days, which oversaturates the ground is also another cause of Floods. All rivers in Canada experience flooding specially due to temperature fluctuation and ice/snow melting [23].Fires, and landslides are in the medium probability category and are not in the top threats that a business have to worry about but has to be for sure considered.

Human Error

The interesting issue associated with misconfiguration is that even if an enterprise has the best technologies and disaster recovery solutions in the market, misconfiguration of those technologies due to lack of knowledge or lack of training for employees brings this threat to the high probability category. Having backups audited on a scheduled and random base is a must to make sure that images or complete backups are ready to be restored in a case of a disaster.

Another main threat for Canadian businesses is the lack of trained or educated employees that are willing to work. According to [25], labor shortages in Canada already have pushed wages for some workers as much as sixty percent (60%) higher than their counterparts in the U.S. In other words, Canada is a multicultural country that is continuously accepting immigrants on that basis of knowledge and added value they can acquire when they come to this country. This in fact is due to the reason that there is a crisis in the number of educated and well trained individuals that are ready to work on different shifts (including night shifts and overtime).

Every business undergoes construction once in a while whether it is renovation, changing décor of offices or adding new space. Construction is sometimes lengthy and might take up to months. Any error done by the contractor might significantly affect the work of the whole enterprise. For example. If by mistake a fire sensor was hit when contractor was on site doing work, the fire alarm will go and employees have to evacuate until fire department comes in and make sure it is safe for everyone to be back. If that fire sensor was a water pipe that was mistakenly drilled by contractor, a flood will likely to happen threatening power and heating systems.

IT Related Errors & Other Threats

Heating Outage in a country like Canada where the temperature drops to -40 C in winter is a major problem with a high probability. In December 2013, an ice storm hit the Canadian provinces Ontario, Quebec and New Brunswick leaving residents struggling to stay warm, check on neighbors, clear tree branches, and wait for crews working round the clock to restore power to more than 195,000 homes in Toronto, 58,000 in Ontario, almost 40,000 in Quebec and 44,000 in New Brunswick [26]. Heating is usually based on natural gas or electricity and if any problem leads to delay in heating, pipes will get frozen within few minutes.

Security is divided into two parts, the first covers physical security and the other one is data. Physical security breach or damage is not so probable to occur as Canada is considered a safe place to live and work in. Data security on the other hand is a very high vulnerable aspect that has to be considered when drafting a disaster recovery plan. All security breaches from fake authentication and authorization attempts, brute force attacks using botnets to do a denial of service, social engineering and foot printing to acquire part of the system or database, and insiders being paid to do malicious activities all fall under the security threat.

Pandemic is the third threat under this category which is considered as highly probable according to [23]. When a pandemic like influenza hits; customers, employees, vendors and all stakeholders will be affected.

Explosions as a result of terrorism are considered as a low threat but still has to be considered. The late explosion that took place in Boston while a marathon was happening is a good example on why a Canada Business has to be prepared for those events though North America is considered to be a safe place.

Mitigation

Note: A detailed "Business Scenario Case" section follows this section and discusses the solutions in specific.

This section will emphasize on the solutions given to mitigate the risks associated with the threats mentioned above. To start with, the essential part of this Disaster Recovery Framework's mitigation solutions is building an alternate site to move to in a case of a disaster, "hot, warm or cold site”. Those sites vary largely in terms of the cost since they offer different facilities. A hot site has almost everything that essential and critical operations need to have the work carried on. It is usually costly to have a continuously updated and backed up hot site with employees on call or even attending the site. A warm site is usually a place where there are computers and plugins and employees have to move in to that site that is usually at least 30 Miles away from the actual location of the disaster. A Cold site is essentially an empty building with only basic utilities such as water, and electricity and Internet connection

The first thing that a business have to consider when trying to build a warm site would be the location of this alternate site, keeping in mind that it has to be at least 30 Miles away from the original location.

The warm site that will be proposed in the “Putting this template into a test” section is a solution that any Midsize Canadian business that is willing to spend the same budget can consider. It is a coast to coast solution that might be implemented almost anywhere. The other option that the research is examining; and that is increasingly being implemented, is outsourcing the DR alternate size to a specialized vendor that charges a yearly fee. The numbers of those vendors are significantly increasing according to the limited research done regarding what they offer. The research will show that the cost of building and maintaining a warm site is relatively high as compared to signing an agreement with those vendors. Also, when considering a privately owned warm site, an enterprise has to account the cost of maintaining the site and updating the equipment continuously even if no disaster hits in a given year or years.

To sum up, though the cost of setting up a warm site and owning it is considered a onetime fee; the cost associated with owning such a site has to be well considered. Owning a warm site is a common practice for larger organizations but not medium size ones with limited budget.

Outsourcing data centers is not only the trending solution today; lately, a new idea emerged in the United States of America which is providing portable sites that can be dispatched and brought to the enterprise so that work is carried on until they can recover and go back to the actual location. These sites can be located right next to the actual building in a case of power or system outage, or can be in another city away from the disaster. The impact of the disaster determines whether they are hot, warm or even cold sites. They are efficient solutions for small and medium enterprises because of the relatively low cost. According to the preliminary research done regarding those vendors, none of the Canadian vendors are offering those solutions yet “this might be an excellent idea for an emerging business.

COBIT 5 for Risk

COBIT 5 for risk is considered a guide for risk management and acts as a best practice tool that has to be considered whenever a business is taking its policies and strategies a step further. According to ISACA.org, “Effectively *managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives”*. According to COBIT 5 for Risk, systemized processes are considered essential to sustain, govern and manage the risk. At the second level, information flows; in terms of hierarchy, has to be well set to know who is accountable, responsible, informative, or consultant. Organizational Structures including people and their skills should be put in order whenever an enterprise is considering to develop an effective risk function. This research tackled the important aspects of the COBIT 5 for risk enablers by identifying the risk, giving a template to prepare who is in the position of authority so that he is contacted; according to the RACI model, building the risk scenario, providing solutions that are relevant and affordable and focusing on the testing and training aspect of any policy being implemented.

According to COBIT 5 for Risk, Chapter 3, “*IT risk scenario is a description of an IT-related event that can lead to a loss event that has a business impact, when and if it should occur”*. The generic scenarios serve, after customisation, as input to risk analysis activities.
Below is a table that includes generic risk scenarios “figure 38 in COBIT 5 for Risk document”

- **Risk scenario category** is a high level description of the category of the scenario the research is examining.
- **Risk scenario components** provides details about the threat type, actor, event, asset/resource and time of every scenario category.
- **Risk type**—The type to which scenarios derived from this generic scenario will fit, using three risk types as follows
  1. **IT benefit/value enablement risk**—Associated with (missed) opportunities to use technology to improve the efficiency or effectiveness of business processes or as an enabler for new business initiatives
  2. **IT programme and project delivery risk**—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes
  3. **IT operations and service delivery risk**—Associated with the operational stability, availability, protection and recoverability of IT services, which can bring destruction or reduction of value to the enterprise

NOTE: **‘P’** indicates a primary (higher degree) fit and **‘S’** represents a secondary (lower degree) fit.
Blank cells indicate that the risk category is not relevant for the risk scenario at hand.

Check appendix for complete COBIT 5 mapping[WU8]

The only two risk categories that were not discussed and mapped to the DRP plan are the architecture of the business and regulatory compliance. The size was previously defined as a medium sized business which will provide flexibility when implementing the DRP regardless of the "Architecture" of the organization. Regarding the regulatory compliance, this research is examining the Canadian market from coast to coast, thus the regulations change between each province and another. Also, internal regulations of the business should not be an obstacle or an identified risk since they can be amended to accommodate the DRP proposed plan (see appendix for complete COBIT 5 mapping).

Putting the proposed template to a test

In this section, the research will build a case for a fictitious, Alberta-based enterprise by basing the scenario on the latest Calgary's river flood in 2013; a city wide disaster that affected almost all kinds of businesses including schools and hospitals. Only after that disaster, did the government of Alberta decide to reconsider an effective DRP plan that effectively plans, directs and reacts to such an event [27].

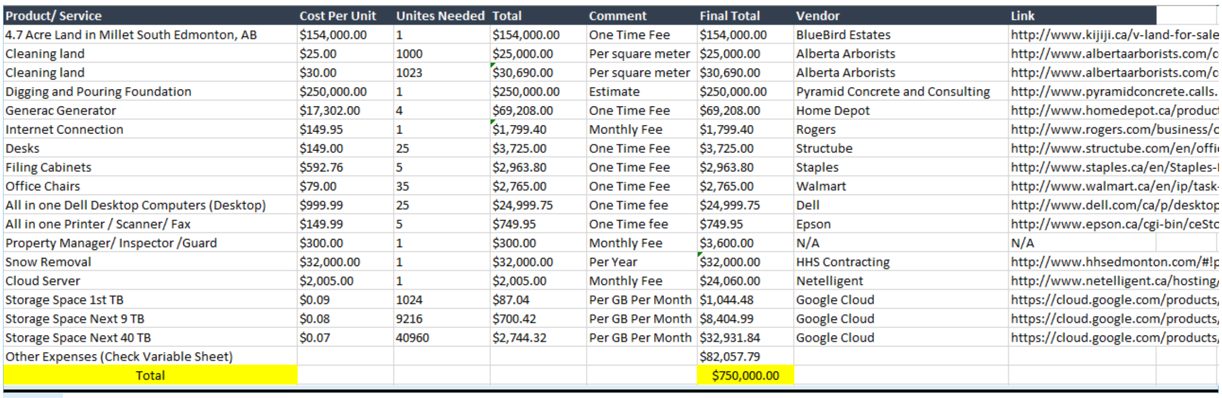
The research will consider that the DRT consist of 30 employees from different departments and will break down the scenario into two options. First option is building a warm site from scratch and the second one is signing an agreement with a third party vendor. The vendor this research is considering has warm sites available in Vancouver, Canada and Toronto Canada [28].

Note: In both options, the research will provide an accounting cost ledger for the first year and then for the recurring years.

To download and view the full excel sheets, please visit https://drive.google.com/file/d/0BxDnXKXRd3npZURtSkprZVZVSHM/edit?usp=sharing

One file with 5 excel sheets is uploaded.

First Option



Product/ Service	Cost Per Unit	Unites Needed	Total	Comment	Final Total	Vendor	Link
4.7 Acre Land in Millet South Edmonton, AB	$154,000.00	1	$154,000.00	One Time Fee	$154,000.00	BlueBird Estates	http://www.kijiji.ca/v-land-for-sale
Cleaning land	$25.00	1000	$25,000.00	Per square meter	$25,000.00	Alberta Arborists	http://www.albertaarborists.com/c
Cleaning land	$30.00	1023	$30,690.00	Per square meter	$30,690.00	Alberta Arborists	http://www.albertaarborists.com/c
Digging and Pouring Foundation	$250,000.00	1	$250,000.00	Estimate	$250,000.00	Pyramid Concrete and Consulting	http://www.pyramidconcrete.calls.
Generac Generator	$17,302.00	4	$69,208.00	One Time Fee	$69,208.00	Home Depot	http://www.homedepot.ca/product
Internet Connection	$149.95	1	$1,799.40	Monthly Fee	$1,799.40	Rogers	http://www.rogers.com/business/c
Desks	$149.00	25	$3,725.00	One Time Fee	$3,725.00	Structube	http://www.structube.com/en/offi
Filing Cabinets	$592.76	5	$2,963.80	One Time Fee	$2,963.80	Staples	http://www.staples.ca/en/Staples-I
Office Chairs	$79.00	35	$2,765.00	One Time Fee	$2,765.00	Walmart	http://www.walmart.ca/en/ip/task-
All in one Dell Desktop Computers (Desktop)	$999.99	25	$24,999.75	One Time fee	$24,999.75	Dell	http://www.dell.com/ca/p/desktop
All in one Printer / Scanner/ Fax	$149.99	5	$749.95	One Time fee	$749.95	Epson	http://www.epson.ca/cgi-bin/ceStc
Property Manager/ Inspector /Guard	$300.00	1	$300.00	Monthly Fee	$3,600.00	N/A	N/A
Snow Removal	$32,000.00	1	$32,000.00	Per Year	$32,000.00	HHS Contracting	http://www.hhsedmonton.com/#!p
Cloud Server	$2,005.00	1	$2,005.00	Monthly Fee	$24,060.00	Netelligent	http://www.netelligent.ca/hosting/
Storage Space 1st TB	$0.09	1024	$87.04	Per GB Per Month	$1,044.48	Google Cloud	https://cloud.google.com/products/
Storage Space Next 9 TB	$0.08	9216	$700.42	Per GB Per Month	$8,404.99	Google Cloud	https://cloud.google.com/products/
Storage Space Next 40 TB	$0.07	40960	$2,744.32	Per GB Per Month	$32,931.84	Google Cloud	https://cloud.google.com/products/
Other Expenses (Check Variable Sheet)					$82,057.79		
Total					$750,000.00		

[WU9]

Table 1.1 Building a DRP that includes a warm site from scratch- First Year Cost Sheet

In the scenario this research is examining, the actual location of the business is in the core downtown of Edmonton, Alberta while the alternate site would be in Millet, AB. Millet is 55 KM away from Edmonton's south (a 45 minute drive) and on the highway that connects the two major cities Edmonton and Calgary in Alberta.

First assumption: 4.7 acre land located in Millet on major route "45 Ave"
Cost: $ 154, 000
Cost Type: Onetime fee
Vendor: Blue Bird Estates
Facilities provided: Power and phone connections available to site.

Second assumption: Cleaning land and preparing it to be built.
Cost: $ 55,690 for half an acre ($25 per meter square for the first 1000 Meter square / additional $5 thereafter)
Cost Type: One Time
Vendor: Alberta Arborists
Facilities provided: Cutting trees down, flattening surface, land mowing and removing junk and grass.

Third assumption: Digging and pouring foundation for a two story medium size building with office spaces and basement.
Cost: $ 250,000
Cost Type: One time
Vendor: Pyramid Concrete
Facilities provided: Excavation, digging, hauling dirt, and pouring concrete foundation.

Fourth assumption: Two standalone generators that work on natural gas are placed in actual site and another two in warm alternate site.
Total Cost: $ 69,208
Cost Type: One time
Vendor: Home Depot

Facilities provided: Natural gas generators

Fifth assumption: Internet connection at alternate warm site.
Cost: $ 1799.40
Cost Type: Yearly
Vendor: Rogers
Facilities provided: 5 Static IP account

Sixth assumption: Furniture for warm site (Desks + Filing Cabinets + Office Chairs)
Cost: $ 9,453.80
Cost Type: One time
Vendor: Structtube – Staples - Walmart
Facilities provided: (25) 120 CM Metal desk + 5 filing cabinets + 35 office chairs.

Seventh assumption: Twenty five Dell desktops + five all in one printers
Cost: $ 25,750
Cost Type: One Time
Vendor: Dell & Epson
Facilities provided: 4th generation Intel i3 with 6 Gigs of ram and 1 TB Hard Drive

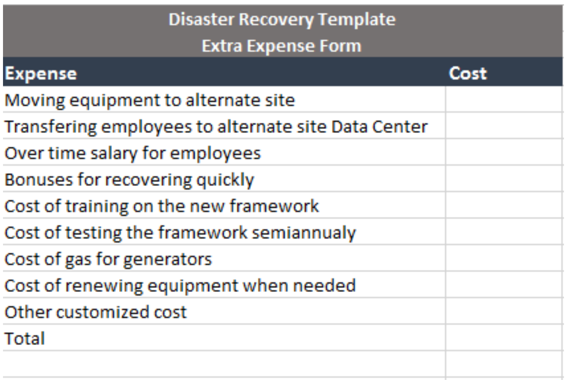
Eighth assumption: Virtual Computing Power
Cost: $ 24,060
Cost Type: Yearly
Vendor: netelligent.ca
Facilities provided: 21.3GHZ VCPU, 25 GB of base RAM, 72 GB of virtual RAM, 750MB/s port speed, 200GB SATA virtual HDD that is backed up daily with a cap of 200 GB + 200GB SAS Virtual HD backed up daily

Ninth assumption: Virtual Storage Space
Cost: $ 42,381
Cost Type: Yearly
Vendor: Google Cloud
Facilities provided: 50 TB of storage space

Tenth assumption: Internet connection at alternate warm site.
Cost: $ 3,600
Cost Type: Yearly
Vendor: N/A
Facilities provided: Inspecting facility on a biweekly basis. Making sure snow removal contractor is conducting work as promised.

Eleventh assumption: Snow removal contractor
Cost: $ 32,000
Cost Type: Yearly
Vendor: HHS Contracting
Facilities provided: Snow removal on a biweekly basis no matter what cm of snow is accumulated.

After having a total expense of $ 632,342.21, Table 1.2 represents a form that can be used to add additional cost that might associate with mitigating any disaster. Table 1.4 is a room to tailor the framework according to the enterprises' specific needs based on different scenarios. Up to $82,057 can be spent during a year on those unaddressed or unexpected costs. Example of those expenses might be extra expense of traveling from original site to the alternate site, training and testing of the framework, paying overtime for staff in addition to moving special equipment that are not available at the alternate site. Also, taxes were not calculated in Table 1.1 since that differs between provinces [29] [30] [31].

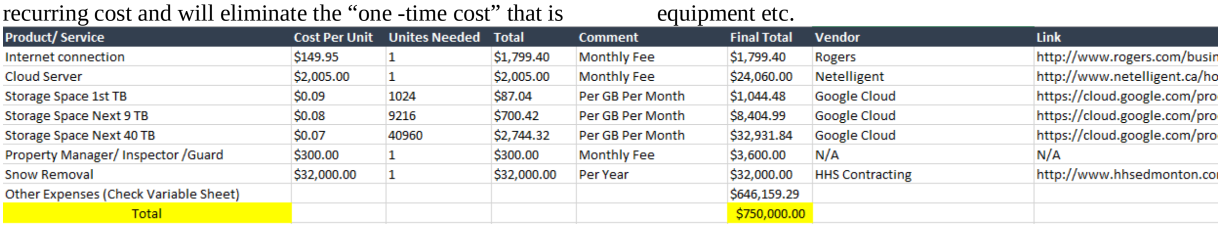


Disaster Recovery Template Extra Expense Form	
Expense	Cost
Moving equipment to alternate site	
Transfering employees to alternate site Data Center	
Over time salary for employees	
Bonuses for recovering quickly	
Cost of training on the new framework	
Cost of testing the framework semiannualy	
Cost of gas for generators	
Cost of renewing equipment when needed	
Other customized cost	
Total	

Table 1.2 Extra Expense Form

First Option – Recurring Years

In this section, the research will shed the light on the yearly recurring cost and will eliminate the "one -time cost" that is associated with buying the land, building it, buying equipment etc.

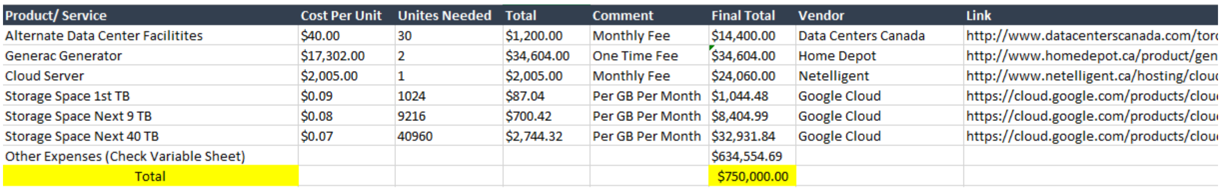


Product/ Service	Cost Per Unit	Unites Needed	Total	Comment	Final Total	Vendor	Link
Internet connection	$149.95	1	$1,799.40	Monthly Fee	$1,799.40	Rogers	http://www.rogers.com/busin
Cloud Server	$2,005.00	1	$2,005.00	Monthly Fee	$24,060.00	Netelligent	http://www.netelligent.ca/ho
Storage Space 1st TB	$0.09	1024	$87.04	Per GB Per Month	$1,044.48	Google Cloud	https://cloud.google.com/pro
Storage Space Next 9 TB	$0.08	9216	$700.42	Per GB Per Month	$8,404.99	Google Cloud	https://cloud.google.com/pro
Storage Space Next 40 TB	$0.07	40960	$2,744.32	Per GB Per Month	$32,931.84	Google Cloud	https://cloud.google.com/pro
Property Manager/ Inspector /Guard	$300.00	1	$300.00	Monthly Fee	$3,600.00	N/A	N/A
Snow Removal	$32,000.00	1	$32,000.00	Per Year	$32,000.00	HHS Contracting	http://www.hhsedmonton.co
Other Expenses (Check Variable Sheet)					$646,159.29		
Total					$750,000.00		

Table1.3 First Option – Recurring years expense cost sheet

The total yearly cost is $ 103,840 and that includes renewing all services ex: internet connection, cloud services, cloud storage in addition to paying the property manager and snow removal contractor the yearly fee. The relatively low yearly cost will give up to $ 646,159 room to expand or customize the plan.

Second Option



Product/ Service	Cost Per Unit	Unites Needed	Total	Comment	Final Total	Vendor	Link
Alternate Data Center Facilitites	$40.00	30	$1,200.00	Monthly Fee	$14,400.00	Data Centers Canada	http://www.datacenterscanada.com/tor
Generac Generator	$17,302.00	2	$34,604.00	One Time Fee	$34,604.00	Home Depot	http://www.homedepot.ca/product/gen
Cloud Server	$2,005.00	1	$2,005.00	Monthly Fee	$24,060.00	Netelligent	http://www.netelligent.ca/hosting/clou
Storage Space 1st TB	$0.09	1024	$87.04	Per GB Per Month	$1,044.48	Google Cloud	https://cloud.google.com/products/clou
Storage Space Next 9 TB	$0.08	9216	$700.42	Per GB Per Month	$8,404.99	Google Cloud	https://cloud.google.com/products/clou
Storage Space Next 40 TB	$0.07	40960	$2,744.32	Per GB Per Month	$32,931.84	Google Cloud	https://cloud.google.com/products/clou
Other Expenses (Check Variable Sheet)					$634,554.69		
Total					$750,000.00		

Table 1.2 DRP Cost Sheet of Signing an agreement with third party vendor

As mentioned earlier; in this section, the research will take into consideration signing an agreement with a third party vendor so that the DRT moves to the rented site whenever a disaster is declared.

First Assumption: Signing an agreement with Data Centers Canada that will provide a fully equipped warm site in case of a disaster so that critical operations are sustained.
Cost: $ 14, 400 ($40 per seat per month for 30 individuals)
Cost Type: Yearly
Vendor: Data Centers Canada
Facilities provided: Shared racks, private racks, private cages and suites. CCTV surveillance, biometric and access card security systems. UPS service, generators that are fuel loaded to last 7 full days.

Second assumption: Two standalone generators that work on natural gas are placed in actual site
Total Cost: $ 34,604
Cost Type: One time
Vendor: Home Depot
Facilities provided: Natural gas generators

Third assumption: Virtual Computing Power
Cost: $ 24,060
Cost Type: Yearly
Vendor: netelligent.ca
Facilities provided: 21.3GHZ VCPU, 25 GB of base RAM, 72 GB of virtual RAM, 750MB/s port speed, 200GB SATA virtual HDD that is backed up daily with a cap of 200 GB + 200GB SAS Virtual HD backed up daily

Fourth assumption: Virtual Storage Space
Cost: $ 42,381
Cost Type: Yearly
Vendor: Google Cloud
Facilities provided: 50 TB of storage space

In the above case, the total expense is $ 115,445 that is considered as a yearly expense except for the Generators part. Table 1.2 represents a form that can be used to add additional cost that might associate with mitigating any disaster and tailor the framework according to the enterprises' specific needs based on different scenarios. Up to $634, 554 can be spent during a year on those unaddressed or unexpected costs.

To download and view the full excel sheets, please visit https://drive.google.com/file/d/0BxDnXKXRd3npZURtSkprZVZVSHM/edit?usp=sharing

One file with 5 excel sheets is uploaded.

Summary & Conclusions

The framework proposed is tailored to Canadian Midsize businesses, acts as a template that can be implemented to any Canadian enterprise with a limited budget. DRP plans should act as a guide for strategic decisions on what technologies are favorable to use. It is an effort to bring practicality and relative affordability to DRP plans in such a way that it gets increasingly implemented in smaller enterprises in Canada. General frameworks on how to implement a disaster recovery plan or on how to effectively react to disasters are already out there to the public. The constraint regarding those documents is that they don't focus on the size or location of business. Mid-size enterprises usually don't have Disaster Recovery professionals on board and would rather send their IT and accounting professionals to conferences or seminars where disaster recovery is being presented so that the latter can acquire the knowledge to be used when considering a new business continuity or disaster recovery plan. Also, when trying to draft a framework that is specific for a certain size of business, it is a better practice to limit the framework's target to a certain geographic location. In other words, what applies to Canada doesn't apply to the Middle East or to the European region especially when it comes to identifying threats and finding solutions available to mitigate the risk. A Mid-size company in Canada for instance differs to that in the states in terms of capital, yearly revenues and yearly profits. The framework, using three percent (3%) of yearly gross revenues, covers most of the threats that are associated with operating in Canada.

Suggestions for Further Research

The proposed framework took into consideration three percent (3%) of yearly gross revenues as a budget for the mitigation solutions provided. Also, the threats were based specifically on the most common Canadian risks and disasters. Further research might reconsider the criteria on how to categorize a business size. Since the budget was based on yearly gross revenues, this budget might change whenever the category of business size changes. Also; new technologies might be launched, that will reduce the cost and propose more efficient solutions. Example on that would be the portable warm sites that are currently not available in Canada.

Example Risk Scenarios

Appendix

		Risk Type			Example Scenarios	
Ref.	Risk Scenario Category	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
1.1	Portfolio establishment and maintenance	**P**	**P**	**S**	Wrong solutions to mitigate risks associated with disasters are selected for implementation that don't align with corporate strategic direction.	Programs lead to successful new business initiative that are cost effective and that add a value.
1.2		**P**	**P**	**S**	Duplication between initiatives (Example: BCM and DRP)	Aligned initiatives.
1.3		**P**	**P**	**S**	New solutions proposed are incompatible with enterprise's hierarchy. Example: DRT privileges.	Assessment and compatibility of all functional units.
2.1	DRP Project life cycle management (Projects initiation, economics, delivery, quality and termination)	**P**	**P**	**S**	Failing of implementing the DRP (due to cost, delays, scope creep, and change in business priorities) project not terminated.	Scope Creeps of implementing DRP project are corrected and aligned with business priorities
2.2		**S**	**P**	**S**	DRP project budget overrun	The project meets budget guidelines
2.3		**S**	**P**		Late delivery of certain solutions by vendor	Delivery is on time
3.1	IT investment decision making	**P**		**S**	Business managers are not involved in important BCM and IT related investment decision making (e.g., new applications, prioritisation, and new technology opportunities).	There is co-ordinated decision making over the DRP investment between decision makers
3.2		**P**		**S**	The wrong proposed software, in terms of cost, performance, features, and compatibility is selected for implementation.	Upfront analysis is performed and a business case is made up to ensure the adequate selection of software/infrastructure.
3.3		**P**		**P**	The wrong infrastructure, in terms of importance to carry on critical tasks are selected to be available in proposed warm site.	
4.1	IT expertise and skills	**P**	**P**	**P**	There are insufficient skills to participate in the DRT.	Correct skill mix and training ensures that there is a thorough understanding of the plan by staff
4.2		**P**	**P**	**P**	There is a lack of due diligence in the recruitment process of the DRT.	Candidates are screened to ensure that appropriate skills are met.
4.3		**P**	**P**	**P**	There is a lack of training leading to staff not participating in the BCM project.	Staff members are able to determine their own training plan based on domain of interest.

5.1	Staff Operations	**P**	**S**	P	Theft of device with sensitive data while moving to warm site, theft of key infrastructure component.	Premises and equipment are monitored and secure even while transferring to other locations
5.2		S	S	P	Access rights of DRT are abused	Coordination on frequent basis to ensure timely removal of access rights.
5.3		S		P	Information is input incorrectly by DRT	The four eye principle is applied.
6.1	Information (data breach: damage, leakage and access)	S		P	Database is corrupted leading to inaccessible data	Backup procedures are aligned to business criticality of data and are virtually accessible.
6.2		**P**		S	Portable media containing sensitive media is lost at time of disaster	Portable media is properly secured and encrypted.
6.3		**P**		**P**	Sensitive information is disclosed using email or social media at time of disaster	Employees are aware of social media usage policy.
7.1	Infrastructure (hardware and operating System)	**P**	S	**P**	New equipment installed at warm site resulting in an unstable transition	Appropriate testing conducted in testing phase.
7.2		**P**	**P**	**P**	Systems at warm site cannot handle transaction volumes	
8.1	Software	**P**		S	Immature DRP solutions (Not fully tested, bugs, early adopters)	
8.2		**P**		S	Application software being used at actual site is obsolete (Hard to move to warm site)	Virtualization fully implemented
8.3		**P**		S	Unintentional modification or configuration error	The 4 eye principle is applied.
9.1	Ownership of DRP Plan	**P**	**P**	S	Business does not assume accountability over new technologies of BCM/DRP plans.	Business assumes appropriate accountability.
9.2		**P**	S	S	Inadequate requirements lead to ineffective service level agreements with vendors.	
10.1	Supplier selection/ performance, contractual compliance, termination of service and transfer		S	p	There is a lack of supplier due diligence regarding delivery capability and sustainability of service.	Third party acts as strategic partner.
10.2			S	p	Outsourcer performance is inadequate in a large-scale long-term outsourcing arrangement.	Appropriate key performance indicators (KPIs), linked to rewards and penalties, ensure adequate service delivery and support.
10.3			S	p	There is an inability to transfer to alternative suppliers due to overreliance on current supplier.	A phase-out and knowledge transfer clause is added to the contract with the supplier
11.1	Geopolitical			p	There is no access due to disruptive incident in other premises.	Clear compliance with national policies and support of local initiatives ensures support by local government and generation of business value
11.2				p	Government interference in a case of an emergency and national policies limit service capability	
11.3				p	Targeted action against the enterprise results in destruction of infrastructure.	

12.1	Infrastructure theft or destruction	S	S	P	There is a theft of a device with sensitive data.	Key infrastructure components are monitored 24/7 for performance, availability.
12.2		S	S	P	.There is a theft of a substantial number of development servers.	
13.1	Malware	**S**		**P**	There is an intrusion of malware on critical operational servers.	IT infrastructure will be appropriately protected behind firewalls on the warm site premises and through continuous monitoring of the network to ensure the execution of day-to-day activities.
13.2		**S**		**P**	Regularly, there is infection of laptops with malware.	
13.3		**S**		**P**	A disgruntled employee implements a time bomb that leads to data loss.	
13.4		**S**		**P**	Company data are stolen through unauthorised access gained by a phishing attack.	
14.1	Logical Attacks	P		P	Unauthorised users try to break into systems.	
14.2		S		P	There is a service interruption due to denial-of-service attack.	
14.3		S		P	The web site is defaced.	
14.4		S		P	Industrial espionage takes place.	
14.5		S		P	There is a virus attack.	
14.6		S		P	Hacktivism takes place.	
15.1	Industrial Action	S	S	P	Facilities and building are not accessible because of a labour union strike.	A business continuity plan foresees action to be taken to always ensure the execution of business critical tasks in case the building is not accessible anymore.
15.2		S	S	P	Key staff is not available through industrial action (e.g., transportation strike).	A flexible work policy, allowing employees to work from another location than the office building simulates freedom and creates a positive work atmosphere.
15.3		S	S	P	A third party is not able to provide services because of strike.	

16.1	**Environmental**	S	S	**P**	The equipment used is not environmentally friendly (e.g., power consumption, packaging).	Being awarded for environmental friendliness creates positive media attention, attracts new customers and employees, and ensures value creation.

17.1	**Acts of nature**	S	S	**P**	There is an earthquake.	
17.2		S	S	**P**	There is a tsunami.	
17.3		S	S	**P**	There are major storms and tropical	
17.4		S	S	**P**	There is a major wildfire.	
17.5		S	S	**P**	There is flooding.	
17.6		S	S	**P**	The water table is rising.	

18.1	**Innovation**	**P**	**S**	**P**	New and important technology trends are not identified.	Innovation and trend watch are endorsed and encouraged.
18.2		**P**		S	There is a failure to adopt and exploit new software in a timely manner.	
18.3		**P**		S	New and important software trends are not identified.	

Bibliography

[1] T. Lock, B. Bennett and D. Vile, "Disaster Recovery in European SMBs," *FreeForm Dynamics,* October 2011.

[2] S. Widup, "Business Continuity Planning in Difficult Economic Times," *SANS Institute Infosec Reading Room.*

[3] Statistics Canada, "http://www.statcan.gc.ca," 22 June 2012. [Online]. Available: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/econ166a-eng.htm.

[4] Canada, Industry, "Key Small Business Statistics - August," 2013.

[5] S. Balaouras, "Building The Business Case For Disaster Recovery Spending," 3 April 2008. [Online]. Available: http://www.qad.com/Public/Collateral/Forreste_BuildingCasefor_DR_040308.pdf.

[6] R. DINES, "The State Of Disaster Recovery Preparedness," 6 January 2011. [Online]. Available: http://www.drj.com/2011-articles/winter-2011-volume-24-issue-1/the-state-of-disaster-recovery-preparedness.html.

[7] J. Kavur, "IT World Canada," 29 June 2009. [Online]. Available: http://www.itworldcanada.com/article/symantec-releases-worldwide-disaster-recovery-statistics/37020.

[8] FEMA, "National Disaster Recovery Framework," 2011.

[9] Symantec, "SMB Disaster Preparedness Survey," Global Results, 2011.

[10] V. Kopytoff, "Bloomberg Business Week Technology," 4 December 2012. [Online]. Available: http://www.businessweek.com/articles/2012-12-04/the-importance-of-disaster-plans.

[11] H. Hamidovic, "An Introduction to Incident Preparedness and Operational Continuity Management Based ISO/PAS 22399:2007," *ISACA Journal,* p. Volume 3, 2011.

[12] C. A. Johnson, "Understanding Recovery Point Objective (RPO)," November 2008. [Online]. Available: http://www.tug.ca/articles/Volume24/V24N2/TUG_V24N2_05-08_Johnson.pdf.

[13] ISACA, "http://www.isaca.org," *Major Planning Considerations Checklist,* pp. 7-22.

[14] J. P. Pironti, "Key Elements of an Information Security Program," *ISACA Journal,* p. Volume 1, 2005.

[15] Symantec, "Disaster Preparedness Survey," 2012.

[16] J. McKendrick, "Cisco: Cloud Will Soon Handle Most Data Center Workloads," 4 December 2011. [Online]. Available: http://news.yahoo.com/cisco-cloud-soon-handle-most-data-center-workloads-040712886.html.

[17] J. F. Kovar, "8 Surprising Disaster Recovery Stats," 2012.

[18] Quality Technology Solutions Inc., "10 Steps to Implement a Disaster Recovery Plan".

[19] G. Sanders, "Rimpa.com.au," 2004. [Online]. Available: http://www.rimpa.com.au/assets/2011/02/BusinessC

ontinuityPlan.pdf.

[20] Sungard Availability Services, "THE BUILDING BLOCKS FOR A SUCCESSFUL RECOVERY PROGRAM," 2013. [Online]. Available: http://www.sungardas.com/Documents/disaster-recovery-plan-template-SFW-WPS-086.pdf.

[21] Admin Service, "BASIC DISASTER RECOVERY & CONTINGENCY PLAN," [Online]. Available: http://www.formsmax.com/download/disaster-recovery-plan-template-3.html.

[22] NIST 800-34, "Contingency Planning Guide for Federal Information Systems," May 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

[23] C. RedCross, "Common Emergencies and Disasters," 2013.

[24] R. L. Jones, "CANADIAN DISASTERS - AN HISTORICAL SURVEY," 2013. [Online]. Available: http://web.ncf.ca/jonesb/DisasterPaper/disasterpaper.html.

[25] Bloomberg News , "Canada’s labour shortage threatens $50B LNG plans," 9 December 2013. [Online]. Available: http://business.financialpost.com/2013/12/09/canadas-labour-shortage-threatens-50b-lng-plans/?__lsa=91db-2bb9.

[26] S. Boesveld, "Hundreds of thousands still without power across Toronto and Eastern Canada 48 hours after massive ice storm," 23 December 2013. [Online]. Available: http://news.nationalpost.com/2013/12/23/hundreds-of-thousands-still-without-power-across-toronto-and-eastern-canada-48-hours-after-massive-ice-storm/.

[27] CBC News, "http://www.cbc.ca/," 11 July 2013. [Online]. Available: http://www.cbc.ca/news/canada/calgary/alberta-flood-area-building-rules-may-change-says-redford-1.1308059.

[28] D. C. Canada, "Data Centers Canada," 2013. [Online]. Available: http://www.datacenterscanada.com/.

[29] Bell, "Putting the cloud to work for your organization".

[30] H. Depot, "GENERAC," [Online]. Available: http://www.homedepot.ca/product/generac-60-kw-natural-gas-liquid-cooled-standby-generator/921052.

[31] G. C. Services, "Google Cloud," [Online]. Available: https://cloud.google.com/products/cloud-storage/?utm_source=google&utm_medium=cpc&utm_campaign=cloudstorage-search&gclid=CO3C4ciFmb0CFcURMwodemMALA.

[32] The Globe and Mail, "www.theglobeandmail.com," 27 June 2013. [Online]. Available: www.theglobeandmail.com/report-on-business/rob-magazine/top-1000/top-1000/article12829649/.

[33] ISACA, "A Strategic Framework for IT Disaster Recovery Assessments," *ISACA Journal,* p. Volume 6, 2012.

[34] M. Brogan, "Will your Business survive the next Disaster ?," *Edge Business,* May 2010.

[35] K. Parris, "Who Survives Disasters and Why, Part 2 : Organizations," 2010.

[36] C. Mullen, "Business Planning for Disaster Survival".

[37] Brandpoint (ARA), "http://www.dailyhome.com," 2013.

[38] S. R. N. a. R. W. Owens, "http://web.ebscohost.com," 2 September 2013. [Online]. Available: http://web.ebscohost.com/bsi/pdfviewer/pdfviewer?sid=371eb509-d205-478f-8fc3-f95e975874da%40sessionmgr15&vid=6&hid=25.

[39] K. Casey, "57% Of SMBs Have No Disaster Recovery Plan," *Information Week,* 11 January 2011.

[40] O. D. W.-. XTIUM, Composer, *Buidling a Framework for an Effective Disaster Recovery Plan.* [Sound Recording]. 2014.

[41] Tower Stream, "Minimizing the Risk of Unplanned Downtime by Ensuring Redundancy," [Online]. Available: http://www.towerstream.com/docs/redundancy.pdf.