BUSINESS IMPACT ANALYSIS REPORT

Company: Grey County
Date: April 8th, 2019
Version: DRAFT

Perry Group Consulting Ltd.

The Objectives

Grey County IT ("IT") supports a variety of business applications, such as VOIP phones, accounting, document management, websites, GIS, asset management, email, HR systems, as well as systems and applications related to patient care at three long-term care homes and a network of paramedic services. These services extend across 95 virtual servers (Windows 2003-2016, Linux), and support over 25 physical locations.

As such, it is the IT departments responsibility to ensure continued delivery of technology services to the County's critical business functions in the event of a disruption. As part of the IT departments Disaster Recovery and Resiliency Initiative, Business Impact Analysis (BIA) and [1]Risk Assessments were conducted. The results of which are the primary content of this document.

The BIA process is more than just a checkbox in the annual list of business continuity program activities. When done correctly, it can provide useful information to drive continuous business continuity program improvement and ensure a more prepared organization. Some causes of a poor BIA include:

1. **Failing to distinguish enterprise applications:** Some applications are more important than others because they serve the enterprise as a whole. Therefore, there is no one business manager who can state the overall importance of those applications. However, an application that serves a single business function, or that serves many functions in different ways may not be as readily noticed. There are some applications such as a payroll application or customer relationship management (CRM) systems whose impact is self-evident. But there are others (e.g., legal support, document management) that may go relatively unnoticed.

2. **Failing to recognize data centre applications:** Some applications do not have business users. These applications include the operating systems, database management systems and data centre tools that enable business applications. It is easy to say that all of the infrastructure must be recovered before all applications, but should the operating system on an obscure server that performs analysis really be recovered before the credit, trading or inventory systems?

3. **Pre-determining BIA results:** Sometimes the result of an analysis seems obvious to business managers, so they automatically assume the answer without going through the BIA process. Assumptions may yield correct results 80% of the time, but that means they're incorrect 20% of the time. In other words, one out of every five business functions or applications is inaccurately analyzed. The impact may only become apparent when a disaster strikes, and by then it is too late.

The purpose of a BIA is to pinpoint which business units or departments, operations and processes are crucial to the continued delivery, and in some cases, uninterrupted delivery of technologies and services to the organization. The primary purpose of this BIA is to identify critical technologies and services IT delivers to the County. While this effort was intended to focus on technologies, Perry Group Consulting ("PGC") used the opportunity to identify non-technical information that is of importance to Business Continuity Planning (BCP) for each County department.

It should be noted that Long Term Care (LTC) was treated as a unique in that a separate risk assessment was performed in order to identify risks specific to the three facilities supported by IT.

---

[1] **Risk** *is a function of the values of threat, consequence, and* **vulnerability***. The objective of* **risk management** *is to create a level of protection that mitigates* **vulnerabilities** *to threats and the potential consequences, thereby reducing* **risk** *to an acceptable level.*

The main objectives of this Business Impact Analysis were to:

1. Identify all business functions within each department
2. Assign each function a Recovery Time Objective with justification
3. Identify the applications supporting those business functions
4. Assign application criticality based upon their respective business function
5. Identify upstream and downstream dependencies that may affect the delivery of goods and/or services.

The technical information gathered will be used to develop disaster recovery strategies for the County. All non-technical information has been made available to the County departments for Business Continuity Planning (BCP) purposes.

A terminology list can be found in APPENDIX A - Terminology

Methodology, Discovery, Assumptions and Constraints

Methodology

PGC chose to use interviews and impact categories/criteria as a means of collecting information. Interviews provide a more reliable and comprehensive method of gathering information than a survey. Further, interviews provide an opportunity for increasing the level of awareness and departmental responsibility for response and recovery planning.

PGC interviewed a selection of department heads, direct reports, and functional managers. Upon completion of the interviews, the data gathered from each of the three levels were cross checked for thoroughness, consistency, and to uncover missing or relevant information, and then uploaded to the PGC portal for processing.

The interview consisted of a series of questions to identify functions, criticality, dependencies, legal and regulatory requirements, key personnel, alternate locations, and other technical and non-technical information.

The assigned criticality is from the users' perspective only. Further fine tuning will occur over time and applications will change as IT becomes more mature in its resiliency efforts.

Upstream and Downstream Dependencies

In addition to the direct impact of a business disruption such as an ice storm or flood, there are also indirect impacts the have been considered in this BIA. These are viewed as upstream and downstream dependencies. Upstream dependencies refer to impacts the County will suffer if a services external to a department or the company as a whole is affected by a service outage.

If a company relies on regular deliveries of products or services by another third-party company, that company could experience upstream losses if that third-party cannot deliver. Internally, an isolated service outage in a specific department may in fact impact the delivery of one or more services in other departments within your organization. This is how a disaster elsewhere can impact you, even if your company or department is unaffected.

For the purpose of this BIA, each County departmental service will list all other County services that rely on that particular service to function. i.e. downstream dependencies

Upstream Dependency Breakdown

In considering the complexity of dependencies, a traditional BIA approach typically fails to consider IT service management (ITSM) best practices (e.g. ITIL) and most certainly the proliferation of cloud services over the last few years. With that in mind, PGC has added an additional level of detail specific to upstream dependencies that has allowed the County to clearly identify service dependencies in the following categories:

Information Technology	External Departments	Cloud Services	External Partners
IT service catalogue	other corporate services	external cloud services	third-party vendors/suppliers

Impact Categories

Impact categories are the aspects of your business that you will be looking at to determine the negative effects of disruptions of varying lengths. There is no universal list of impact categories that works in all industries. Rather, every organization chooses a few such categories based on its unique situation. For the County BIA five impact categories were used for each business unit. The Health & Safety category replaced Operations for both Long Term Care and Paramedic services.

For financial impact the County selected the following thresholds to determine impact level:

Level 1	Level 2	Level 3	Level 4	Level 5
$0 - $25,000	$25,000 to $50,000	$50,000 to $100,000	$100,000 to $250,000	Over $250,000

Qualitative and Quantitative Impacts

A BIA can utilize both a qualitative and quantitative approach.

Quantitative impact can be measured, often in financial terms. For example, when IT systems fail, the quantitative impact to the business may be defined in terms of:

- Salaries paid to an idle workforce that depends on an application
- Penalties and fines for missed deadlines

Qualitative impact refers to losses or consequences that are less tangible and difficult to assign an immediate monetary value. For example, when IT systems fail, the qualitative impact to an organization could be defined in terms of:

- Loss of reputation or damage to the brand because your banks network was down for a few hours while processing payroll
- Political or public embarrassment resulting from an IT system failure during a high-profile product launch

Table 1 details the various impact categories used during the BIA process.

Table 1 - BIA Impact Categories

[2]Financial	Reputation (Image Credibility)	Operational (Service Delivery)
▪ Loss of business ▪ Increase in operating costs ▪ Cash flow impact ▪ Loss of productivity (idle workers) ▪ Fines ▪ Late fees ▪ Emergency purchases	▪ Loss of credibility ▪ Damage to public image or confidence due to lack of service delivery ▪ Decreased employee morale ▪ Political embarrassment or damage due to reduced public service, image, or confidence	▪ Degraded customer service ▪ Degraded public service ▪ Loss of personnel ▪ Loss of management control
Legal & Regulatory	**Health & Safety**	**Contractual**
▪ Breach of law ▪ Legal liability ▪ Noncompliance with Government regulations	▪ Loss of life ▪ Safety risk ▪ Health risk	▪ Noncompliance with third-party contracts and SLA's

[2] **Validating financial impact thresholds**: an often over-looked component of the process includes discussing with executive management the thresholds of pain that could be associated with a disaster. Asking the question as to whether a $5M loss or a $50M loss would have a significant impact on the long-term bottom line of the organization can lead to interesting results. We need to understand what financial impacts are acceptable or unacceptable to the organization.

Discovery

Interviews were conducted beginning August 29th, 2018 and were completed by December 20th, 2018. Upon completion of each interview, a summary was sent to the interviewee for review and approval. A follow-up review was scheduled which was then incorporated into his/her departmental BIA report. The BIA was then published on the portal for review with members of the IT team. The BIA Final Report was compiled using the information from the departmental reports. Department and individual BIA Summaries are available through the portal.

Assumptions and Constraints

The BIA was constructed by the information elicited from the end users. It is assumed that the end user knows best which applications are critical to their business functions.

- A BIA is only the first of several steps in determining the criticality of Customer applications/functions. The BIA reflects the opinions of the end users. Criticality of County applications will be fine-tuned when the Disaster Recovery Plan (DR) and the Business Continuity Plans (BCP) are developed and tested.
- The BIA alone cannot be the only factor in determining appropriate recovery strategies. When selecting the appropriate strategy, each application requires all three of the following:
    1. [3]Data sensitivity
    2. Level of criticality
    3. Cost of recovery strategy

Because the BIA was a project of and for IT, the BIA was focused on County technologies. When able, additional non-technical information was gathered on behalf of the Departments. The PGC portal should be leveraged and updated as required, since it is expected that further information will be gathered as part over an overarching business continuity program.

During the course of the project, the IT department implemented a core piece of technology that has provided an improved level of performance and availability (hyperconvergence) to the compute/storage infrastructure. This system needs to be formally documented and included as part of the IT disaster recovery plan.

[3] PGC conducted a high-level (sample) assessment of data sensitivity (Engineering folder) in order to assist in the initiation of a formal data classification program. The results of this assessment have been detailed in this report.

Recovery Time Objectives (RTO)

The business functions and supporting applications of Grey County have been assigned a level of criticality referred to as RTO or Recovery Time Objective tier.

An RTO level is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. As outlined in Table 1, five tiers of criticality were defined based on the process of determining mission essential functions as per the guidelines provided by PGC.

Table 2 – Service Criticality Tiers and Criteria

RTO Tier	Recovery Objective	Criteria
Tier 1	0-4 hours	Assigned to business functions that are **critical** to the operations of the organization or support matters of life and death.
Tier 2	24 hours	Assigned to **urgent** functions that directly support tier 1 functions or would have a significant impact to revenue, customer service, and/or brand image.
Tier 3	3 days	Assigned to **important** functions that can be restored after tiers 1 and 2 have been restored.
Tier 4	7 days	Assigned to **normal** functions that can be deferred until more critical County functions have been recovered. Most County functions fall within levels 4 and 5
Tier 5	2-4 weeks	Assigned to functions that are considered "**non-essential**" to the core business (low priority).

The assignment of criticality to each function was determined based on the RTO above, the expertise within the department, industry expertise, and generally accepted practices within the industry.

Most downtime events are not the result of total devastation. However, for response and recovery planning purposes, a worst-case scenario is used. A worst-case scenario assumes that the physical infrastructure supporting each respective business unit has been destroyed and all records, equipment, personnel, etc. are not immediately accessible. In the event of total municipal devastation, the rebuild efforts would exceed the RTOs and by extension the Maximum Tolerable Downtime (MTD) for critical business services.

The RTOs above should be re-evaluated to meet the requirements of the technology capabilities on a regular basis and with each change to the production operating environment or methodology.

If the capabilities of technology do not meet the requirements of the business unit, a gap exists leaving the business unit vulnerable. These gaps must be identified and mitigated to prevent extended outages and serious impact to the County. Some gaps are discovered while conducting the BIA but a more thorough discovery of vulnerabilities are revealed during the testing and validation of the departmental business continuity plans and the Disaster Recovery Plan (DRP). Testing and validation of BCP and DR plans should be done annually (at a minimum).

Departmental Impact

Interview Schedule

Table 3 – Departmental Interview List

Department	Primary Contact
• County Clerks	Heather Morrison
• Economic Development	Savana Myers
• Emergency Systems	Marlene McLevy
• Finance	Kevin Weppler
• Grey Roots Museum	Petal Furness
• Housing	Anne Marie Shaw
• Human Resources (HR)	Sandra Shipley
• Long Term Care	Lynne Johnson
• Paramedic Services	Kevin McNab
• Planning	Randy Scherzer
• Provincial Offences Court	Amanda Kokas
• Social Services	Barb Fedy
• Tourism	Bryan Plumstead
• Transportation (Engineering)	M.Marck
• Transportation (Maintenance)	Graham Wilson

Service Criticality Ratings (0-3 Days)

Based on data collected from interviews with business units - not meeting the recovery time objective (RTO) for each specific service…

Department/ Business Process	Will…				
			Downtime Factors		
	Impact Assessment	Impact	RTO Score	RPO	MTD
Long-Term Care/ Communication	… have a negative impact on safe resident care, medication delivery, therapeutic menus and diet orders, physician orders, resident need/tasks, allergies, fall risk, and responsive behaviours.	Very High	**188 0-4hrs**	1-Day	1-Day
Long-Term Care/ Staff Management	… risk loss of staff resulting in degradation of life safety services.		**141 0-4hrs**	1-Day	1-Day
Long-Term Care/ Resident Care	…result in the inability to contact families/emergency contact for items such as updates on resident location	Very High	**132 0-4hrs**	1-Day	3-Days
Paramedic Services/ Non-Emergency Trans.	… risk the transportation to the hospitals/medical facilities for booked/special appointments (i.e.: CT scan at Owen Sound hospital).	Very High	**132 0-4hrs**	1-Day	3-Days

Based on data collected from interviews with business units - not meeting the recovery time objective (RTO) for each specific service…

Department/ Business Process	Will…		Downtime Factors		
	Impact Assessment	Impact	RTO Score	RPO	MTD
Paramedic Services/ Emergency Response	… risk emergency response services to the public/patients and transport to the hospitals for further medical attention.	Very High	**132 0-4hrs**	1-Day	1-Day
Paramedic Services/ Community Paramedic	… risk services to patients in our Community Paramedic program; visiting patients in home to improve health and welfare.	Very High	**132 0-4hrs**	1-Day	1-Day
Paramedic Services/ Scheduling	… risk scheduling of staff responsible for life-safety of residents.	Very High	**132 0-4hrs**	1-Day	2-Days
Emergency Systems/ Emergency Operations	…result in a chaotic and less efficient response to, and management of, the emergency which could result in loss of life, injury, property damage and losses, and long term psychosocial and economic damages to the community due to the, as well as a loss of confidence in the County government.	Very High	**124 0-4hrs**	1-Day	1-Day
POC/Court Proceedings	… result in not fulfilling legal obligation to provide defendants the option to contest any provincial offences charges - 11b Charter rights-times frames.	Very High	**115 0-4hrs**	1-Day	3-Days
Transportation(Main)/ Road Safety	… allow for the potential of unsafe roads, not following Ontario Minimum maintenance standards. Consequences could include injuries, fatalities, and liability / litigation.	Very High	**101 0-4hrs**	1-Day	3-Days
Paramedic Services/ Public Access Defib. Program	… limit support to the PAD program; ensure maintenance of equipment is completed, tracks serial numbers, where they are located and expiry dates of supplies.	Very High	**100 0-4hrs**	1-Day	3-Days
Social Services/ Ontario Works	… risk people in position of not having enough money for food or shelter unable to obtain coverage for medical needs.	Very High	**84 0-4hrs**	1-Day	3-Days
Transportation (Main)/ Traffic Lights	… risk safety to road user, traffic control. Consequence: liability and risk of litigation if signals were inoperable during an accident.	Very High	**83 0-4hrs**	1-Day	3-Days

Based on data collected from interviews with business units - not meeting the recovery time objective (RTO) for each specific service…

Department/ Business Process	Will…		Downtime Factors		
	Impact Assessment	Impact	RTO Score	RPO	MTD
Housing/ Community Housing	… result in the unavailability of Emergency After Hours Services which could have a major adverse effect on family's and damage the County's reputation.	High	**72 24hrs**	1-Day	3-Days
Social Services/ Fee Subsidy Program	… result in the failure to issue subsidy approval in a timely manner which in turn could result in disruption of service/care for residents of Grey county.	High	**68 24hrs**	1-Day	3-Days
Social Services/ Home Child Care	… risk an impact on serious occurrence reporting.	High	**68 24hrs**	1-Day	3-Days
Transportation Eng./ Traffic Signals (Main.)	… risk liability and litigation if signals were inoperable during an accident.	Medium	**57 3-days**	1-Day	5-Days
Housing/ Homelessness Programs	… risk inability for clients to reach programs.	Medium	**56 3-days**	1-Day	5-Days
POC/ Legal Applications	… risk legal obligation to provide defendants the option to contest any provincial offences/charges.	Medium	**54 3-days**	1-Day	5-Days
Human Resources/ Payroll	… result in staff not getting paid, grievances from union, damage to reputation. Could have financial penalties related to employee debts.	Medium	**51 3-days**	1-Day	5-Days
LTC/ Food Ordering (Dietary)	… risk delivery, therapeutic menus and diet orders.	Medium	**51 3-days**	1-Day	5-Days
LTC/ Meal Planning & Delivery	… risk delivery of resident meals.	Medium	**46 3-days**	1-Day	5-Days
Finance/ Accounts Receivable	… result in inability to track required information for Ministry to support transfer payments.	Medium	**45 3-days**	1-Day	5-Days
Transportation Main/ Accident Response	…risk safety to road users.	Medium	**41 3-days**	1-Day	5-Days

Application Summary

The fundamental task in a business impact analysis (BIA) is understanding which business processes are vital to the ongoing operations of the business and to understand the impact a disruption of these processes would have on the business. From an IT perspective, as the [4]National Institute of Standards and Technology (NIST) views it: "The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components." So, there are two parts to the BIA: the first is to understand mission-critical business processes and the second is to correlate those to IT systems.

There were four primary purposes of the business impact analysis for:

1. Obtain an understanding of the County's most critical objectives, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.
2. Inform a management decision on Maximum Tolerable Outage (MTO) for each function.
3. Provide the resource information from which an appropriate recovery strategy can be determined/recommended.
4. Outline dependencies that exist both internally and externally to achieve critical objectives.

The applications list in the BIA contains only those [5]internal applications that have been identified by the end users as being critical to service(s) availability; these applications have been added to the IT Service Catalogue. There were 13 core applications identified (including email and enterprise content management). There is an extensive list (121) of both internal and cloud-based applications that needs to be further reviewed in order to ensure all applications and dependencies have been identified. It is safe to assume that any missing applications can be considered as "noncritical". If any of the applications not mentioned are in fact critical, their criticality will be reveled in the DR plan and BCP plans.

Application RTO's

Internal Applications

Prior to the BIA process, the County had gathered a list of 121 corporate applications (including IT) which were published in a separate spreadsheet. During the course of the BIA process the applications in *Table 4* were highlighted as critical to the business. It is expected that additional applications may be identified through further investigation.

Table 4 – Internal Application Criticality List

Application Breakdown by Criticality			
Application	**Description**	**RTO**	**Notes**
Application Services (Wanderguard)	System running at LTC facilities		**At risk (no redundancy)**
Application Services (Nurse Call)	System running at LTC facilities		**At risk (no redundancy)**
Database Services (PostgreSQL)	Database required for core applications		

[4] Source: NIST "Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, p.16
[5] PGC created an IT Service Catalogue for the County to capture all core services/applications delivered to the business. All external "cloud" based services have been identified in a separate "Cloud Services Catalogue" as outlined in this report.

Application Breakdown by Criticality			
Application	**Description**	**RTO**	**Notes**
Database Services (MariaDB)	Database required for core applications		
Email	Corporate email		Exchange
ECM (Alfresco)	Content management system core for most services		
Application Services (Emergency Contacts)	Emergency Management		
Application Services (Emergency Management Portal)	Emergency Management		
Application Services (Corporate Website)			Recommend outsource to third-party
Application Services (Siemens BAS)	HVAC Systems		Grey Roots Museum [6](FACILITY SYSTEM)
Database Services (MSSQL)			
Application Services (Bellamy)	Work Management		
Application Services (POA Dashboard)	Court Proceedings		
Application Services (Great Plains)	ERP		
Application Services (OCCMS)	Ontario Child Care		
Application Services (Council Expense)	HR Software		
Application Services (GIS)			
Application Services (SRM)			
Application Services (HRWare)	HR Software		
Application Services (CAMs)	Court Proceedings		
Application Services (Inspections Reporting)	Engineering (TS)		
Application Services (Worksheets)	Community Housing		
Application Services (Tweedsmuir Web Service)	Public Information System		
Application Services (Capital Projects)	Financial Reporting and Budget		

[6] Facility system(s) will be treated independent of business systems

Cloud Applications

In considering the extensive adoption of cloud-based services experienced by most organizations as of late 2018, PGC has developed a separate category to capture third-party cloud services considered to be "in-scope" as part of a disaster recovery strategy (*Table 5*) i.e. at least one business unit relies on the cloud service to deliver a service captured in the BIA.

PGC also recommends that all cloud services be catalogued in a separate sub-section of the overarching IT Service Catalogue. Cloud services should be separated into at least [7]two distinct groups:

1. **Customer-facing Services (Cloud)** - any cloud-based service that a "business service" relies on to meet RTO requirements
2. **IT Supporting Services (Cloud)** – IT supporting services such as Mobile Device Management (MDM) being delivered by a third-party cloud provider

Table 5 – Cloud Application Criticality List

Cloud Service Catalogue	Tier 1 (0-4 hours)	Tier 2 (24-hours)	Tier 3 (3-days)	Tier 4 (7-days)
AmbulanceDispatch(FatPot)				
AssetAuction(GovDeals)				
BedTransfers(PTAC)				
Communication(Skype)				
DaycareProvidorDiscovery(ONEHSN)				
DeathRecords(ServiceOntarioFormsPortal)				
DrugInformationService(Pepid)				
EmergencyVolunteerManagement(SAVE)				
EMSDocumentManagement(iMedic)				
FoodOrdering(SyscoPortal)				
FoodService(SyscoSynergy)				
GIS(ESRI)				
HealthRecords(eConnect)				
ICON2.0(French Trial Notices)				
LTCResidentTestResults(LifeLabs)				
MandatoryReporting(LTCHomesDotNetPortal)				
OnlineBanking(TD)				
PatientHealth(PointClickCare)				
PharmacyForms(ClassicCare)				
PropertyManagement(Yardi)				
RemotePatientMonitoring(IdealLife)				
ResidentWaitingListandApproval(CCACPortal)				
RideCoordination(TripSpark)				
RoadCompliance(Oscar)				
RoadConditions(Wood)				
Scheduling(StaffScheduleCare)				

[7] A recommended third group would be cloud services not necessarily part of the DRP requirements, but services that consume bandwidth and host corporate data

BIA Value Add

- Information gathered will help assist the IT team to fine tune the Master Applications List and to manage County applications going forward.
- The BIA methodology was designed to encourage ongoing communication and collaboration of BCP and DR planning efforts with County departments.
- The BIA was designed to help transfer and/or share BCP and DR ownership and subsequently costs to Customers.
- On behalf of the customers, IT gathered non-technical information the departments can use to update or develop their BCP plans
- IT has a better understanding of which departments use/share a single application, e.g., Great Plains is used by HR, Finance, POC, and Housing.
- IT will able to track more thoroughly the impact of changing or decommissioning applications. In addition, IT is better able to prevent the procurement of redundant software packages.
- Through the BIA, IT is able to identify applications that are supported externally. This will help in transitions from externally supported applications to IT supported applications & services.

Threats, Vulnerabilities, and Risk

A disaster recovery [8]risk assessment and business impact analysis (BIA) are crucial steps in the development of a disaster recovery plan. Once you've compiled your business impact analysis, the next step is a risk assessment. An IT risk assessment is a process that describes potential threats your organization faces, whether they are natural and/or man-made. These threats are weighed by the likelihood of occurrence and then multiplied by their effect on the operation. The result is a value that you can use to determine your level of protection against a threat and identify any vulnerabilities that require attention.

It is akin to an eye-opening exercise; a good risk analysis and assessment helps throw insight into how each functional area of a business would be impacted in the event of a disaster and therefore, it also helps in prioritizing recovery plans based on the criticality of the functions.

In terms of how we treat these risks, we can use the following categorization:

- **Prevent:** High-probability/high-impact events (actively work to mitigate these)
- **Accept:** Low-probability/low-impact events (maintain vigilance)
- **Contain:** High-probability/low-impact events (minimize likelihood of occurrence)
- **Plan:** Low-probability/high-impact events (plan steps to take if this occurs)

The approach taken by PGC was to separate Corporate Administration, LTC and Grey Roots Museum to perform standalone assessments for each of these areas. Results automatically generated an online heat map and risk register to be utilized as part of an overarching Business Continuity Plan (BCP). As illustrated in *Figure 1*, there were a number of medium-level risks that will require further follow-up. Although a select number of concerns within these categories have been flagged, this report is primarily focused on high-level risks with associated vulnerabilities.

[8] Risk = The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability

VALUE SCORECARD

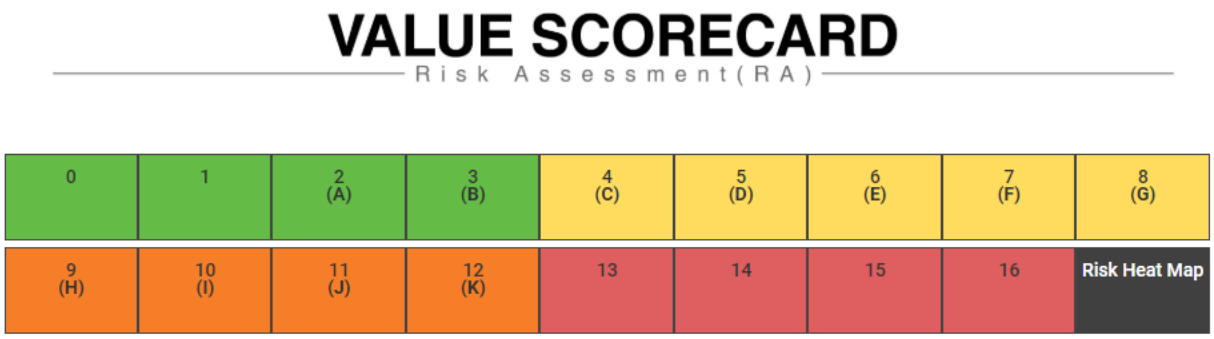
Risk Assessment (RA)

0	1	2 (A)	3 (B)	4 (C)	5 (D)	6 (E)	7 (F)	8 (G)
9 (H)	10 (I)	11 (J)	12 (K)	13	14	15	16	Risk Heat Map

Letter	Threat (Category)	Rank
A	Nature (Environmental)	2
B	Chemical Spill (Environmental)	3
B	Explosion (Environmental)	3
B	Forest Fires (Environmental)	3
B	Hurricane/Tornado (Environmental)	3
B	Fire (Environmental)	3
C	Loss of Staff (Human)	4
C	Climate and Contamination (Facility (Grey Roots Museum))	4
D	Power Failure (Environmental)	5
D	Loss of Hardcopy Records (Infrastructure & Location (LTC))	5
E	Unauthorized Access to Senstive Data (Human)	6
E	Flood (Environmental)	6
E	Physical Forces (Facility (Grey Roots Museum))	6
E	Ice Storm (Environmental)	6
F	Flood (Water) (Facility (Grey Roots Museum))	7
F	Fire (Facility (Grey Roots Museum))	7
F	Malicious Software Upload (Human)	7
G	Physical Security (Location)	8
G	Unintentional Action to Sensitive Data (Human)	8
G	Physical Security (Infrastructure & Location (LTC))	8
G	Cybersecurity (Infrastructure)	8
G	Security (Facility (Grey Roots Museum))	8
G	Cybersecurity (Infrastructure & Location (LTC))	8
G	Security Lifecycle (Infrastructure & Location (LTC))	8

Figure 1 - Risk Assessment (Low/Medium)

There were numerous high-risk threats/vulnerabilities identified for both Grey County Administration and LTC facilities (as outlined in Figure 3).



Letter	Threat (Category)	Rank
H	Identification & Authentication (Infrastructure & Location (LTC))	9
H	Sensitive Data (Infrastructure & Location (LTC))	9
H	Sensitive Data (Infrastructure)	9
H	Identification and Authentication (Infrastructure)	9
H	System and Data Integrity (Infrastructure)	9
H	Security LIfecycle (Infrastructure)	9
I	Network and Computer Based Attacks (Human)	10
I	System & Data Integrity (Infrastructure & Location (LTC))	10
I	Business Continuity & Disaster Recovery (Infrastructure & Location (LTC))	10
I	Logging and Audit (Infrastructure)	10
I	Business Continuity and Disaster Recovery (Infrastructure)	10
J	Network Resiliancy (Infrastructure & Location (LTC))	11
J	Network Resiliancy (Infrastructure)	11
J	Logging and Audit (Infrastructure & Location (LTC))	11
K	Loss of Hardcopy Records (Location)	12

Figure 3 - Risk Assessment (High)

For the purpose of this document a selection of high-level threats/vulnerabilities (IT specific) outlined in *Figure 3* have been analyzed and categorized into five areas as follows:

1. Policy & Organizational (IT)
2. Network Resiliency
3. Network Management
4. Security
5. Business Continuity/DR

Policy & Organizational Risks (IT)

R1 RESOURCE LIMITATIONS	
Probability	High
Impact	High
Vulnerabilities	V36. Loss of Staff V37. Cross-Training
Affected Assets	A1. Company Reputation A3. Employee Loyalty & Experience A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A20. Certification
Risk	**High**
Comments	There are critical (life-safety) systems dependant on 1 or 2 resources supporting a large percentage of the IT infrastructure. With a "keeping the lights on" approach there is a significant risk if one of these resources is not available to support an issue with any of these systems. The issue is exacerbated when considering the system resiliency vulnerabilities.

R2 ACCOUNT & DEVICE MANAGEMENT	
Probability	High
Impact	High
Vulnerabilities	V1. Identification V3. Protection V9. System Access V7. Cybersecurity Training V17. Asset Management
Affected Assets	A1. Company Reputation A4. Intellectual Property A5. Personal Sensitive Data A6. Personal Data A12. Credentials
Risk	**High**
Comments	Policies are not in place that require employees to lock or log off unattended systems, or to educate users on the risks of theft and/or loss of system. There are also no procedures in place for revoking access for departing employees. Users may also have access to systems and data not appropriate to their duties since titles change but access is not always reviewed.

Network Resiliency

R3 CORE NETWORK (ADMINISTRATION BUILDING)	
Probability	High
Impact	High
Vulnerabilities	V18. High Availability V22. Single Point of Failure V23. Contract Management
Affected Assets	A1. Company Reputation A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A17. Physical Hardware
Risk	**High**
Comments	If there is a SAN or switch failure in the core the entire network environment will fail. There is maximum capacity on host servers with no redundant nodes. Some core equipment is very old and needs to be replaced (maintenance an issue) Most UPS systems are very old any not under warranty.

R4 CORE NETWORK (LTC FACILITIES)	
Probability	High
Impact	High
Vulnerabilities	V18. High Availability V22. Single Point of Failure V23. Contract Management
Affected Assets	A1. Company Reputation A2. Company Trust A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A17. Physical Hardware
Risk	**High**
Comments	There is a single VMware host at all 3 facilities with no redundancy This is a major risk for core applications: Nurse Call, WanderGuard, ShoreTel phone system. Switches are very old (being replaced). There is visible damage to equipment (Rockwood) due to water leaks. Most UPS systems are very old any not under warranty. LTC will also be affected by a SAN or switch failure in the core (entire network environment will fail).

Network Management

R5 CONFIGURATION MANAGEMENT	
Probability	High
Impact	High
Vulnerabilities	V18. High Availability V29. Backup
Affected Assets	A1. Company Reputation A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A17. Physical Hardware
Risk	**High**
Comments	As of April, 2019 SonicWall GMS needs to be fixed. If this is done then configurations will be backed up, but at this point in time it appears to be a vulnerability.

R6 LIFECYCLE MANAGEMENT	
Probability	High
Impact	High
Vulnerabilities	V18. High Availability
Affected Assets	A1. Company Reputation A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A17. Physical Hardware
Risk	**High**
Comments	Most UPS systems are very old any not under warranty. In general, much of the equipment is old and unstable.

R7 CHANGE MANAGEMENT	
Probability	High
Impact	High
Vulnerabilities	V13. Change Management
Affected Assets	A1. Company Reputation A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A17. Physical Hardware
Risk	**High**
Comments	There are no change logging processes in place e.g. changes to devices are automatically or manually logged including date, time, user name, and reason for change. Changes to essential systems are not tested in non-production environments before being implemented into the primary environment. No change management in place.

R8 RELEASE MANAGEMENT	
Probability	High
Impact	High
Vulnerabilities	V18. High Availability
Affected Assets	A1. Company Reputation A3. Employee Loyalty & Experience A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections etc.) A20. Certification
Risk	**High**
Comments	Operating systems and applications are not updated with current security patches within a reasonable time frame. Have some windows 2003 servers and access 97 databases that are in production and not supported by the vendor.

Security

R9 SENSITIVE DATA (BREACH)	
Probability	High
Impact	High
Vulnerabilities	V1. Identification V2. Classification V3. Protection V4. Data Loss Prevention V5. Sensitive Media Sanitization
Affected Assets	A1. Company Reputation A2. Company Trust A4. Intellectual Property A5. Personal Sensitive Data A6. Personal Data A7. Personal Data Critical A9. Service Delivery – Real Time A10. Service Delivery
Risk	**High**
Comments	The County has no policies/procedures in place dictating where/how sensitive data is stored or transmitted. Some users are signing up for cloud services without consulting IT or the clerk's office.

R10 CYBER ATTACK (BREACH)	
Probability	High
Impact	High
Vulnerabilities	V1. Identification V2. Classification V3. Protection V4. Data Loss Prevention V18. High Availability
Affected Assets	A1. Company Reputation A2. Company Trust A4. Intellectual Property A5. Personal Sensitive Data A6. Personal Data A7. Personal Data Critical A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections)
Risk	**High**
Comments	Currently the VPN allows non-domain computers to connect to most admin building resources, requiring only username/password with no 2 factor or device authorization. The DMZ between the pubic and corporate network needs to be analysed (currently any/any/any to/from LANs). No policies/procedures in place dictating where/how sensitive data is stored or transmitted. Some users are signing up for cloud services without consulting IT or the clerk's office.

Business Continuity/DR

R11 BCP/DR PLANNING	
Probability	High
Impact	High
Vulnerabilities	V29. Backup V30. Planning V31. Asset Inventory V32. Testing
Affected Assets	A1. Company Reputation A2. Company Trust A4. Intellectual Property A5. Personal Sensitive Data A6. Personal Data A7. Personal Data Critical A9. Service Delivery – Real Time A10. Service Delivery A16. Network (connections) A17. Physical Hardware A18. Physical Building
Risk	**High**
Comments	The technology aspect of the BCP/DR plan is a work in progress, but there still needs to be an overarching BCP.

R12 BACKUP/RECOVERY (TESTING)	
Probability	High
Impact	High
Vulnerabilities	V1. Identification V2. Classification V3. Protection V4. Data Loss Prevention V5. Sensitive Media Sanitization
Affected Assets	A1. Company Reputation A2. Company Trust A4. Intellectual Property A5. Personal Sensitive Data A6. Personal Data A7. Personal Data Critical A9. Service Delivery – Real Time A10. Service Delivery
Risk	**High**
Comments	The County has no policies/procedures in place dictating where/how sensitive data is stored or transmitted. Some users are signing up for cloud services without consulting IT or the clerks office.

Summary

This BIA is the most critical step in moving the County toward resiliency. Subsequently, the phases toward resiliency heavily rely on the completion of the BIA with each subsequent step building upon the prior phase. Resiliency maturity will not be realized until all phases are complete.

The following diagram (*Figure 4*) represents the County's maturity level (post-PGC engagement) and identifies steps to be taken in order to mature to a level of 4-5.

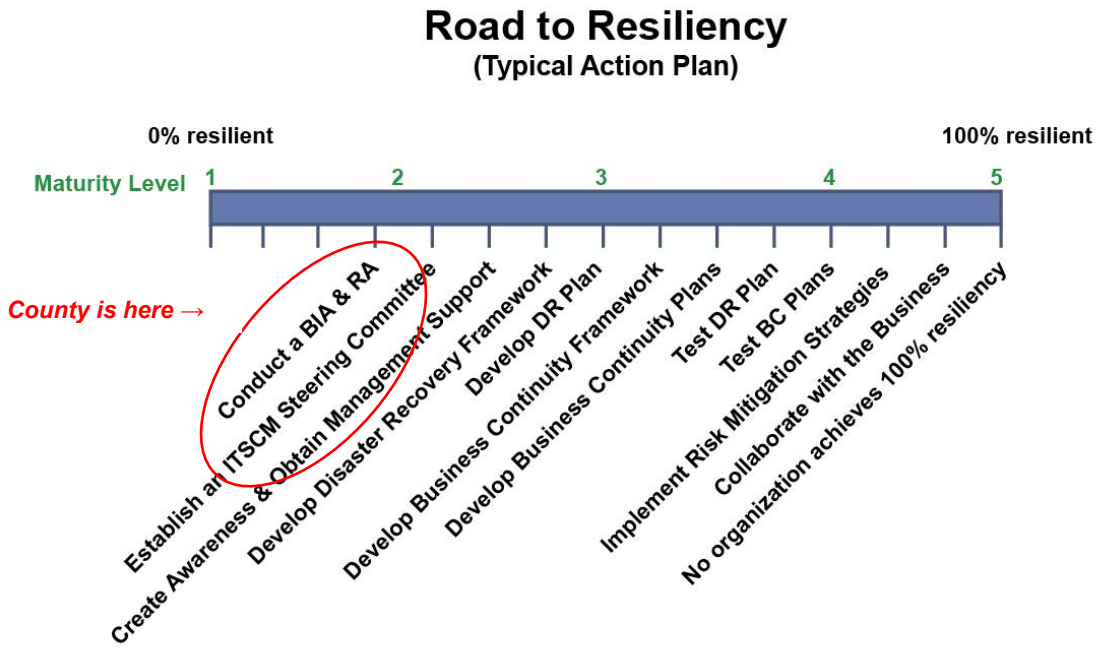


Figure 4 - Road to Resiliency

The County cannot currently recover its technology infrastructure in an acceptable period of time for any critical applications listed in this report.

Many applications are public safety apps, however, there are many core business services that cannot be down (0-4 hours downtime.

For example, the enterprise content management system (Alfresco) is critical to over 90% of the Tier 1 and 2 systems.

5 next steps that are key for the County include:

1. Developing an RFQ/RFP for the procurement of a DRaaS partner
2. Procuring a DR service (DRaaS)
3. Addressing the vulnerabilities listed in this report
4. Initiating an ITSCM Steering Committee
5. Review current BCP posture and leverage PGC findings in this report

Strategic Opportunities

IT Service Catalogue – Core Services

The results of the Business Impact Analysis (BIA) process was used to identify the [9]core IT services required to meet the recovery time objectives defined for each of the County's business services. The IT services listed in *Table 6* should be considered "mandatory" as part of a disaster recovery strategic roadmap, however not all services are considered to be "essential" to the business:

Table 6 - IT Service Catalogue (Core Services)

IT Service Catalogue – Critical Services
Recovery Time Objective (RTO):

0-4 hours	<24 hours	3-days	7-days	2-4 weeks

IT Service	Description	RTO	Service Location
Network Access	Access and authentication to the corporate network		Administration Building (Primary Datacenter)
Network Access (EMS/OW Private Circuit)	Critical (IP) circuit used to communicate with the province		Administration Building (Primary Datacenter)
Telephony (Phone System)	ShoreTel (IP-internally) – PBX on VMware with a Bell PRI uplink		All Facilities
Telephony (Cellular)	iPhones, Androids, other?		N/A
Internet/Intranet	Corporate Internet/Intranet		Administration Building (Primary Datacenter)
Print/Fax Services	Corporate printers		All Facilities
Email	Microsoft Exchange		Administration Building (Primary Datacenter)
ECM (Alfresco)	Enterprise Content Management		Administration Building (Primary Datacenter)
Application Services (Nurse Call)	Critical life safety system		LTC Facilities
Application Services (Wanderguard)	Critical life safety system		LTC Facilities
Application Services (Corporate Website)	Corporate website		Administration Building (Primary Datacenter)
Application Services (Emergency Contacts)	Required for emergency operations		Administration Building (Primary Datacenter)
Application Services (Emergency Management Portal)	Required for emergency operations		Administration Building (Primary Datacenter)

[9] PGC has defined "Core" IT services as those requiring recovery within 3-days of an outage. IT services falling outside of this threshold will be classified in lower t

IT Service Catalogue – Critical Services
Recovery Time Objective (RTO):

0-4 hours	<24 hours	3-days	7-days	2-4 weeks

IT Service	Description	RTO	Service Location
Database Services (MSSQL)	Microsoft database		Administration Building (Primary Datacenter)
Database Services (PostgreSQL)	Open source database		Administration Building (Primary Datacenter)
Database Services (MariaDB)	Open source database		Administration Building (Primary Datacenter)
Network Access (POA Private Circuit)	Critical circuit for POA (serial link between County and Province)		Administration Building (Primary Datacenter)
Application Services (POA Dashboard)	Required for court proceedings and trial scheduling		Administration Building (Primary Datacenter)
Application Services (Bellamy)	Time tracking for Paramedics and Transportation		Administration Building (Primary Datacenter)
Application Services (Great Plains)	ERP – used my several business units		Administration Building (Primary Datacenter)
Application Services (OCCMS)	Child care management		Administration Building (Primary Datacenter)
Application Services (Council Express)	Council meetings (Clerks)		Administration Building (Primary Datacenter)
File Services	Secondary location for file services (should be investigated)		Administration Building (Primary Datacenter)
Application Services (GIS)	Used for civic addressing		Administration Building (Primary Datacenter)
Application Services (SRM)	Currently hosted within County datacenter		Administration Building (Primary Datacenter)
Application Services (HRWare)	HR software		Administration Building (Primary Datacenter)
Application Services (CAMs)	Court Proceedings software		Administration Building (Primary Datacenter)
Application Services (Inspections Reporting)	Road Safety reporting tool		Administration Building (Primary Datacenter)
Application Services (Worksheets)	Community Housing		Administration Building (Primary Datacenter)
Application Services (Tweedsmuir Web Services)	Public information systems (Grey Roots)		Administration Building (Primary Datacenter)
Application Services (Capital Projects)	Financial Reporting and Budget		Administration Building (Primary Datacenter)

IT Services/Application Refinement

A further breakdown of IT services was performed in order to identify applications that were either identified as cloud migration candidates, or not considered "essential" to the business. These applications are highlighted in *Table 7* and *Table 8.* In addition, *Table 9* lists all core in-scope applications

Table 7 - Cloud Migration Candidates

Cloud Migration Candidates		
Application	Status	Recommendation
Microsoft Exchange (email)	County has approved a plan to migrate to O365 in 2019	Migrate to O365 and remove from scope of DR strategy
Corporate Website	Currently hosted within County datacenter	Migration of corporate website to third-party cloud provider – remove from scope of DR strategy

Table 8 - Non-Essential Applications

Non-Essential Applications		
Application	Status	Recommendation
File Services	Currently hosted within County datacentre. Primary application for file services is Alfresco which has been identified as a "core" application	Further review may be required to ensure that files critical to the DR process are not being stored on corporate file servers
Application Services (GIS)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (SRM)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (HRWare)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (CAMs)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (Siemens BAS)	Currently hosted within County datacenter	Further review is required
Application Services (Inspections Reporting)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (Worksheets)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (Tweedsmuir Web Services)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy
Application Services (Capital Projects)	Currently hosted within County datacenter	Consider "out-of-scope" for phase 1 DR strategy

Table 9 - Core Applications (In-Scope)

Core Applications (in-scope for DR strategies)		
Application	Details	Comments
Network Access	Users require access to applications at time of disaster (TOD)	Will be provisioned via SSL VPN or similar at TOD
Network Access (EMS/OW Private Circuit)	Critical private circuit	Options need to be assessed including SD WAN services
Telephony (Phone System)	Users require phone systems at TOD	Assess hardware redundancy of ShoreTel systems and possible SIP trunking (Internet)
Internet/Intranet	Users require access to third-party cloud applications via Internet	Easily provisioned via third-party public WiFi
Print/Fax Services	Users will require access to printers at TOD	Printer redirection a requirement at TOD – assess functionality needs
ECM (Alfresco)	Enterprise Content Management system holding critical files	Standard application recovery requirement
Application Services (Nurse Call)	Life safety system residing at LTC facilities	Low latency layer-2 connectivity dependant on MAC addresses
Application Services (Wanderguard)	Life safety system residing at LTC facilities	Low latency layer-2 connectivity dependant on MAC addresses
Application Services (Emergency Contacts)	Required for emergency operations	Standard application recovery requirement
Application Services (Emergency Management Portal)	Required for emergency operations	Standard application recovery requirement
Database Services (MSSQL)	Several applications require access to this database	Standard database recovery requirement
Database Services (PostgreSQL)	Several applications require access to this database	Standard database recovery requirement
Database Services (MariaDB)	Corporate website + permit payments require access	DR solution may depend on Corporate website migration
Network Access (POA Private Circuit)	Critical circuit for POA (serial link between County and Province)	Option to develop a recovery plan with other municipalities
Application Services (POA Dashboard)	Required for court proceedings and trial scheduling	Standard application recovery requirement
Application Services (Bellamy)	Time tracking for Transportation	Standard application recovery requirement
Application Services (Great Plains)	ERP – used my several business units	Standard application recovery requirement
Application Services (OCCMS)	Child care management	Standard application recovery requirement
Application Services (Council Express)	Council meetings (Clerks)	Standard application recovery requirement

IT Disaster Recovery Tiers

Once the business value of the County's services was determined, data and applications required to delivery each service were assigned a recovery tier based on criticality. A three-tier approach was defined as follows:

Tier 1 – Critical	Tier 2 - Essential	Tier 3 - Important
IT services with an RTO <24 hours	IT services with an RTO ≥3 days	IT services with an RTO ≥7 days
Network Access	Application Services (Great Plains)	File Services
Network Access (EMS/OW Private Circuit)	Application Services (OCCMS)	Application Services (GIS)
Telephony (Phone System)	Application Services (Council Express)	Application Services (SRM)
Internet/Intranet		Application Services (HRWare)
Print/Fax Services		Application Services (CAMs)
ECM (Alfresco)		Application Services (Siemens BAS)
Application Services (Nurse Call)		Application Services (Inspections Reporting)
Application Services (Wanderguard)		Application Services (Worksheets)
Application Services (Emergency Contacts)		Application Services (Tweedsmuir Web Services)
Application Services (Emergency Management Portal)		Application Services (Capital Projects)
Database Services (MSSQL)		
Database Services (PostgreSQL)		
Database Services (MariaDB)		
Network Access (POA Private Circuit)		
Application Services (POA Dashboard)		
Application Services (Bellamy)		

Cost Benefit Analysis (DR Options)

In December, 2018 a cost-benefit analysis was performed to facilitate the financial evaluation of different strategic DR options, with an objective of balancing the cost of each option against the perceived savings. For the purpose of this exercise, three "disaster recovery as a service"(DRaaS) providers were analyzed against the cost and potential benefit of the County building their own DR target within an existing County-owned facility.

With respect service offerings obtained from the DRaaS vendors, in order to qualify as a viable option, the following 5 criteria must have been met:

Requirement #1
Vendor datacenter must be within Canada
Requirement #2
Vendor provides elastic/scalable solution - includes orchestration at time of disaster (TOD) and Failback.
Requirement #3
Pricing must include costs to onboard the County e.g. initial migration services
Requirement #4
Pricing must include all storage and compute costs to protect and deliver in-scope County workloads
Requirement #5
Pricing must meet a realistic anticipated annual budget for the County's business continuity strategy

Vendor Analysis Process

- PGC approached [10]three DRaaS vendors, each with highly rated services within the Canadian DRaaS market (customer recommendations)
- The vendors were <u>not</u> given specifics on "who" the pricing was for other than the actual recovery needs (a sample configuration was used for pricing purposes)
- Vendors were asked to provide costs for implementation, hosting, recovery, and any other ancillary costs associated with the service
- The sample configuration was sent to each vendor
- Vendors were permitted to contact PGC with questions and/or clarification requirements
- Each vendor was given three days to provide an estimate based on County requirements

Note: PGC is recommending that the County perform an analysis on actual compute and storage needs, including confirmation on the actual minimal service levels (MSL ***for example:*** it will need to be determined minimum staff required to perform a business function that requires access to the DR site. The BIA has provided a good baseline by which the County can continue to perform ongoing analysis'.

[10] This report has de-identified vendor details in order to ensure a fair evaluation process

Vendor Analysis Results

Vendor analysis performed in December, 2018 using an initial configuration baseline of: • Total users requiring access at TOD: 400 • Total VMs: 30 • Compute/Storage: 70CPU, 324GB RAM, 20TB Disk		Requirement Met Fully Partial Not Met
Vendor #1		
Requirement #1	Vendor owns their own Tier3+ datacenter located in the GTA	
Requirement #2	Vendor has pre-defined compute levels so flexible scalability is limited	
Requirement #3	Onboarding was included (see #5 for costs)	
Requirement #4	All compute and storage costs were presented in the quote	
Requirement #5	Pricing was quite high at $5,300/mth (onboarding was reasonable @ $35,000)	
Notes: Quote and service was well put together, but the pricing and potential for ancillary costs appeared to be out of the expected range to fit within the County's budget. For this reason, Vendor #1 was eliminated as a viable option for the County.		
Vendor #2		
Requirement #1	Vendor presented Microsoft Canadian datacenter (Azure partner)	
Requirement #2	Vendor has flexible compute/storage on demand and orchestration	
Requirement #3	Onboarding was included (see #5 for costs)	
Requirement #4	All compute and storage costs were presented in the quote	
Requirement #5	Pricing was fair at $3,900/mth (onboarding was reasonable @ $30,000)	
Notes: Considering the County's plan to migrate to O365, Azure is an interesting option for DRaaS. This would also allow for seamless migration of future additional production and/or development workloads to Azure. Discounts may also apply with bulk services.		
Vendor #3		
Requirement #1	Vendor leases a Tier3+ datacenter (Toronto) – Veeam is the replication S/W	
Requirement #2	Vendor has flexible compute/storage on demand and orchestration	
Requirement #3	Onboarding was included (see #5 for costs)	
Requirement #4	All compute and storage costs were presented in the quote	
Requirement #5	Pricing was attractive @ $2,571.50/mth (onboarding was low @ $25,000)	
Notes: Quote and service from this vendor had the highest scoring. In addition to the lowest operating and onboarding costs, telephony expertise would be a potential benefit to the County when considering the criticality of phones and private circuits. Having a providing leveraging the same backup/replication software is a bonus. This vendor also had a cap on monthly costs at TOD (the others did not).		

In-House DR Build

When a business relies on its IT infrastructure for critical business operations, keeping the system up and running is essential. Nothing is more catastrophic to a business than an unexpected system outage. As managers create business recovery strategies to protect their businesses from such events, they may consider setting up an in-house recovery center, or 'hot site'. The benefit of this approach is complete control over the recovery environment. But that option can be expensive and complex to manage. Using a commercial hot site provides flexibility and is a more cost-effective solution.

However, in considering the availability of County assets to potentially act as a DR hosting facility, a cost-benefit analysis comparing DRaaS options to a self-managed solution was recommended.

Please refer to *Table 10* for a summary:

Table 10 - DR Pricing Estimate (in-house)

Hardware/Implementation Cost Estimate (one time)		
Item	Quantity	Cost Estimate
Cage around rack	1	$3,000.00
42U enclosed rack	1	$1,422.00
3000VA UPS	1	$3,262.00
PDU unmanaged	2	$530.00
Cooling	1	$4,500.00
VxRail all flash nodes	3	$180,000.00
Fortigate 500E	2	$90,600.00
Misc cables and hardware	1	$500.00
Electrical contractor	1	$1,500.00
TOR switches	2	$20,000.00
[11]Implementation (hours)	250	$10,937.50
Replication software licenses	TBD	TBD
Total Start-up Costs		**$313,764.00**
Operational Cost Estimate (ongoing annual)		
Hardware maintenance (20%)	12	$59,878.40
Annual DR tests (2-days)	1	$1,225.00
Power/Cooling	TBD	TBD
Ongoing support (hours)	120	$5,250.00
Total Operating Costs		**$66,353.40**

[11] Estimate is based on two County resources working part-time over a period of 2-3 months (install, document builds). Annual salary of $70,000.00 was used plus 30% for benefits - $43.75/hr per resource.

Companies often find it takes more time and money to build this kind of center than allowed for. In addition to the obvious costs, such as the purchase of redundant systems for use in recovery, operating a hot site entails many hidden hardware, software and support costs. Of all the recovery options, in-house recovery is the most expensive.

Cost Benefit Analysis Summary & Recommendations

For comparison PGC looked at the total costs over 5-years to coincide with the County's hardware lifecycle process (*Table 10*). The recommendations also considered skillsets, resource availability, infrastructure control, stability, scalability, facility location, and datacenter classification.

Table 11 - Monthly Costs (5-years)

Monthly Costs (over 5 years)	Details	Monthly Costs (Estimated)
In-house (County Datacenter)	Total onetime + operational over 60 months	**$6,335.29**
[12]DRaaS (Vendor #3)	Monthly cost + implementation over 60 months	**$2,989.50**

Summary

Even if the County **doubles the workload** requirement the monthly costs will still be less expensive than an in-house initiative; without the associated risks.

Although it may seem that "controlling" your own DR site makes sense to the business, running a formal DR program requires a substantial work effort from existing resources already bogged down with day-to-day tasks and projects.

In must be noted, that regardless of approach (In-house or DRaaS) SSL VPN + RDP licenses would be recommended for network access at TOD. The County will need to confirm the status of potential existing licenses (RDP) with Microsoft and determine the number required at TOD.

This is another reason why calculating the minimum level of service at TOD is an important factor. i.e. organizations should not assume that recovering 100% of the technology for 100% of the staff at TOD is required.

The BIA resulted in <100 total desktop/laptop devices specified as being "required" at TOD. The largest percentage being in the Social Services department (60+). The exact numbers will change over time with new initiatives and requirements for services etc. The important factor for the County at this time is acquiring funding to initiate **Phase 1** of the recommendations.

[12] **Ancillary Costs** – If the County required vendor assistance at TOD or Failback the estimated costs would be less than $10,000.00 based on discussions with all three vendors included in the pricing exercise.

Recommendations

Making a large investment in the build of a recovery datacenter is not a recommended approach. The County should consider the following strategy in procuring a DRaaS vendor to host and assist in the management of their DR program:

Phase 1

Calculate "actual" compute, storage[13], print (functionality) requirements for the following:
(Tier 1 + Tier 2)

County Application
Print/Fax Services
ECM (Alfresco)
Application Services (Emergency Contacts)
Application Services (Emergency Management Portal)
Database Services (MSSQL)
Database Services (PostgreSQL)
Database Services (MariaDB)
Application Services (POA Dashboard)
Application Services (Bellamy)
Application Services (Great Plains)
Application Services (OCCMS)
Application Services (Council Express)

Notes:

The objective of this phase is to clarify the actual compute/storage, print (functionality) and access requirements at TOD for Tier 1+2 applications that are **currently delivered from the County datacenter.**

Out of scope applications include:

1. MS Exchange (moving to O365)
2. Corporate Website (move to third-party host)
3. Telephony (separate strategy)
4. Wanderguard (separate strategy)
5. Nurse Call (separate strategy)
6. Private Circuits (separate strategy)
7. Siemens BAS Systems (separate strategy)

Network Access at TOD – would be provided using SSL VPN over RDP with any required desktop clients preloaded in DRP images. This would be the recommended approach regardless of "In-house" or "DRaaS" as the solution. A review of RDP licensing (current) vs future DR requirements will need to be performed. Active Directory with 1+ VM(s) would also be configured at the DRaaS site.

Printing at TOD – would utilize printer redirection which allow for County to have options for printing (e.g. home, remote office, etc.)

Tier 3 Services – In order to lower costs, Tier 3 applications running from the County datacenter will be backed-up to DRaaS facility as a **low-cost backup service**. At TOD the County can determine over the initial hours/days of an outage if in fact they will require one or more of these applications to be recovered and delivered within the 7-day+ RTO requirement. The DRaaS provider will provision as needed (usually within 24-hours).

[13] The County needs to analyze unstructured data to determine the "actual" production capacity requirements for DR replication and hosting services. Inactive "stale" data should be considered for offsite archiving.

Phase 2

Telephony - Critical Applications (outside of County datacenter) - Private Circuits.

County Application/Service
Telephony (Phone System)
Application Services (Nurse Call)
Application Services (Wanderguard)
Network Access (EMS/OW Private Circuit)
Network Access (POA Private Circuit)

Notes:

The objective of this phase is to develop a strategy for critical applications running on equipment outside of the County datacenter, telephony systems, and private circuits.

Telephony – The phone systems are currently IP-based ShoreTel devices with NO SIP trunking (Internet). With this configuration all facilities need to ensure **redundancy** with: POE switches, PBX on VMWare systems, switches, and the existing Bell line.

An option to provide a high-level of redundancy would be to migrate to a SIP trunking solution (Internet) with redundant Internet. This would provide the highest level of redundancy for the County.

LTC Applications (Nurse Call & Wanderguard) - Low latency layer-2 connectivity dependant on MAC addresses. These systems could in fact be part of DRaaS solution (should be investigated further as these systems are exposed).

Private Circuit (EMS/OW) – This circuit could in fact utilized software-defined WAN technology, however the Province should be contacted to confirm options.

Private Circuit (POA) - Option to develop a recovery plan with other municipalities needs to be explored.

Appendix A – Terminology

Term	Definition
Alternate Site	A site held in readiness for use during/following an invocation of business or disaster recovery plans to continue urgent and important activities of an organization.
Application Recovery	The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.
Business Continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level. The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Business Impact Analysis (BIA)	Process of analyzing activities and the effect that a business disruption might have on them.
Business Interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization's location.
Call Tree	A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.
Crisis Management	The overall direction of an organization's response to a disruptive event, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate. Development and application of the organizational capability to deal with a crisis.
Datacenter Recovery	The component of disaster recovery which deals with the restoration of data center services and computer processing capabilities at an alternate location and the migration back to the production site.
Declaration (DR)	A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged response and mitigating actions.

Term	Definition
Disaster Declaration	The staff should be familiar with the list of assessment criteria of an incident versus disaster situation established by the BCM or DR Steering Committee and the notification procedure when a disaster occurs.
Disaster Recovery Plan (DRP)	The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort.
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. The facility used by the Incident or Crisis Management Team after the first phase of a plan invocation. An organization must have a primary and secondary location for an EOC in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts.
Incident	An event which is not part of standard business operations which may impact or interrupt services and, in some cases, may lead to disaster. Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
Maximum Tolerable Downtime (MTD)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Qualitative Risk Assessment	The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories (e.g., customer service, regulatory requirements)
Quantitative Risk Assessment	The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations.
Recovery Point Objective	The point in time to which data is restored and/or systems are recovered after an outage. The point to which information used by an activity must be restored to enable the activity to operate on resumption.
Recovery Time Objective	The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. The period of time following an incident within which a product or service or an activity must be resumed, or resources must be recovered.
Risk Acceptance	A management decision to take no action to mitigate the impact of a particular risk.
Risk Analysis	The quantification of threats to an organization and the probability of them being realized.
Risk Appetite	Total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	Overall process of risk identification, risk analysis, and risk evaluation.

Term	Definition
Risk Mitigation	Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner. Activities taken to reduce the severity or consequences of an emergency.
Risk Register	All risks of an organization, listed, ranked and categorized so that appropriate treatments can be assigned to them.
Single Point of Failure	A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative and a loss of that element could lead to a failure of a critical function. Unique (single) source or pathway of a service, activity and/or process; typically there is no alternative, and loss of that element could lead to total failure of a mission critical activity and/or dependency.
Tabletop Exercise	Technique for rehearsing teams in which participants review and discuss the actions they would take according to their plans, but do not perform any of these actions.
Vital Records	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

Appendix B – IT Service Catalogue (Draft)

TYPE: Customer-Facing Services (APPLICATION, TECHNICAL, PROFESSIONAL)

Service Type

Application		Technical	Professional
Application Hosting Services (per system)		Email	Service Level Management
Enterprise Content Management (Alfresco)		Desktop Services	Project Management
		File Services	IT Consulting
		Print/Fax Services	Security Architecture
		Internet/Intranet	IT Architecture
		Service Desk	Architectural Reviews of New Technology
		Remote Access	IT Procurement Services
		Network Access	Application Development
		Backup/Recovery	Application Enhancement
		Telephony (phone system)	Application Maintenance
		Telephony (cellular)	Vendor Relations
		Storage Provisioning	Business Analysis
			Training
			On-Call Support
			Field Support

OUT OF SCOPE - SUPPORTING SERVICES

TYPE: IT Supporting Services (CORE INFRASTRUCTURE, DATA CENTRE, SECURITY)

Service Type

Core Infrastructure	Data Centre	Security
Infrastructure Services (DNS, DHCP)	Facilities Management (power, cooling, space, physical security)	Identity and Access Management (Active Directory)
Network Services (LAN,WAN, WiFi)	Cloud Management	Anti-Virus
Storage Management (SAN,NAS)		Compliance
Compute (Physical/Virtual Servers)		Certificate (RADIUS) NPS
License Management		
Monitoring		

Appendix C – Recommended IT Asset Codes

Asset	Description	Owner (County or Cloud Provider)	Perceived Value (Very Low – Low – Medium – High – Very High)
A1. Company Reputation		County	Very High
A2. Company Trust	Includes goodwill – can be measured by complaints	County	Very High
A3. Employee Loyalty & Experience		County	High
A4. Intellectual Property		County	High
A5. Personal Sensitive Data	As defined by PIPEDA (Canada)	County/Cloud Provider	Very High
A6. Personal Data	As defined by PIPEDA (Canada)	County/Cloud Provider	High (if lost)
A7. Personal Data – Critical	All data included in the Personal Data category according to PIPEDA, and are classified or considered CRITICAL by the County	County/Cloud Provider	High
A8. HR Data	Data that are relevant from an operational perspective, beside the Data Protection requirements	County	High
A9. Service Delivery – Real Time	All those services that are time critical and that need a level of availability close to 100%	County/Cloud Provider	Very High
A10. Service Delivery		County/Cloud Provider	Medium
A11. Access Control/ Authentication/ Authorization		County/Cloud Provider	High
A12. Credentials	Of Clients and Staff that access systems	County	Very High
A13. User Directory (Data)		County	High
A14. Cloud Service Management Interface	This is the interface that manages all of the services provided through a cloud service	County/Cloud Provider	Very High
A15. Management Interface (APIs)		County/Cloud Provider	Medium
A16. Network (connections, etc.)	All network connections	County/Cloud Provider	High
A17. Physical Hardware		County/Cloud Provider	Low/Medium (depends on redundancy)
A18. Physical Building		County/Cloud Provider	High
A19. Application Source Code		County/Cloud Provider	High
A20. Certification	ISO, PCI, DSS, etc.	County/Cloud Provider	High
A21. Operational Logs	Those logs used to sustain and optimise business processes and for auditing purposes	County/Cloud Provider	Medium
A22. Security Logs	Useful as evidence of security breaches and forensics	County/Cloud Provider	Medium
A23. Backup or Archive Data		County/Cloud Provider	Medium

Appendix D – Vulnerability Codes

VULNERABILITY CODES
V1. SENSITIVE DATA VULNERABILITIES: IDENTIFICATION
Sensitive data needs to identified and classified. Locate sensitive data throughout the enterprise. A significant amount of sensitive data in a single location poses a high risk due to damage possible from a single breach.
V2. SENSITIVE DATA VULNERABILITIES: CLASSIFICATION
Data needs to be classified and clearly defined. A classification scheme needs to be established throughout the organization based on criticality and sensitivity. Ineffective classification processes can cost the organization through breaches and lost productivity.
V3. SENSITIVE DATA VULNERABILITIES: PROTECTION
Vital data needs to be identified, and a strategy for protection and recovery developed and maintained in order to mitigate the risk of data loss.
V4. SENSITIVE DATA VULNERABILITIES: DATA LOSS PREVENTION
Data loss prevention tools are critical to identify, monitor and protect data in storage as well as in motion over the network. These tools secure your system against data leaks and protection against unauthorized entry or use.
V5. SENSITIVE MEDIA SANITIZATION
Physical storage resources: a sensitive data may leak because data destruction policies applicable at the end of a lifecycle may either be impossible to implement because, for example, media cannot be physically destroyed because a disk is still being used by another business unit or it cannot be located, or no procedure is in place. A retention and disposition policy must be created that defines the timeframes during which documents for operational, legal, fiscal or historical value must be maintained.
V6. CYBERSECURITY PROGRAM
An organization must identify reasonably foreseeable internal and external risks pertaining to security, confidentiality, and integrity of the information and systems as part of an information security program. The need to shield information from malicious actors is a concern at the highest levels of business and government.
V7. CYBERSECURITY TRAINING
Negligent employees, contractors and third-party vendors represent the cause of over half of all enterprise data breaches.
V8. CYBERSECURITY MATURITY
Independent third-party security assessments are crucial in order to address the adequacy of policies and procedures defined in your organizations cybersecurity program (V6).
V9. SECURITY LIFECYCLE VULNERABILITIES: SYSTEM ACCESS
Sound system access policies and procedures must be in place in order to mitigate the risk of unauthorized access to corporate data.
V10. SECURITY LIFECYCLE VULNERABILITIES: THIRD-PARTY ACCESS
Third-party vendors should have restricted access to systems as defined.
V11. SECURITY LIFECYCLE VULNERABILITIES: PATCH MANAGEMENT
Failure to follow adequate patch management procedures greatly increases the risk of falling victim to a cyber attack or other security breaches. Global ransomware hacks occur daily as a result of poor patch management. These unattended vulnerabilities in IT infrastructure open companies up to numerous security challenges.
V12. SECURITY LIFECYCLE VULNERABILITIES: RESOURCE ALLOCATION
Sufficient resources (both human and financial) are essential to successfully implement security requirements and initiatives. Third-party SME's should be leveraged as required.
V13. IT SERVICE MANAGEMENT VULNERABILITIES: CHANGE MANAGEMENT
When an organization employs a weak change management process, more than just money is going to be lost. In fact, there are both short term and long term, direct and indirect costs to the organization.
V14. IT SERVICE MANAGEMENT VULNERABILITIES: INCIDENT MANAGEMENT
Formal incident management is required in handling any interruptions that occur so as to restore operation /services back to normal [as planned] as soon as possible. The importance is to minimize its impact on business operation/service.
V15. IT SERVICE MANAGEMENT VULNERABILITIES: PROBLEM MANAGEMENT
The ITIL problem management process investigates recurring incidents, the root cause of incidents, and provides a formal focus on incident prevention. Without a formal problem management capability, these activities tend to fall into a black hole.

VULNERABILITY CODES
V16. IT SERVICE MANAGEMENT VULNERABILITIES: KNOWLEDGE MANAGEMENT
Knowledge management is a required discipline that promotes an integrated approach to identifying, capturing, evaluating, retrieving, and sharing all of an enterprise's information assets. These assets may include databases, documents, policies, procedures, and previously un-captured expertise and experience in individual workers.
V17. IT SERVICE MANAGEMENT VULNERABILITIES: ASSET MANAGEMENT
Asset management allows the organization to keep track of all their IT assets. It can tell where the assets are located, how they are used, and when changes were made to them. It is important for a company to implement an asset management system to assist in the monitoring of assets, as well as in the asset recovery process.
V18. SYSTEM AND DATA INTEGRITY VULNERABILITIES: HIGH AVAILABILITY
It is important to ensure critical data is readily available in situations like server crash, breach, or other data disaster.
V19. SYSTEM AND DATA INTEGRITY VULNERABILITIES: ANTI-VIRUS
Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete. It is time to think beyond traditional antivirus.
V20. SYSTEM AND DATA INTEGRITY VULNERABILITIES: INTRUSION DETECTION
The main reason behind the advent of IDS is that firewalls and access control on their own do not provide an adequate defence against attack. Therefore IDS must be used to monitor network assets to detect anomalous behaviour and misuse in network.
V21. SYSTEM AND DATA INTEGRITY VULNERABILITIES: SECURITY MANAGEMENT
Security checks need to be performed periodically on essential, life/safety and private data systems e.g. patch levels, access controls, configuration settings, etc. in order to mitigate the risk of a system outage.
V22. NETWORK RESILIENCY VULNERABILITIES: SINGLE POINT OF FAILURE
Taking the time to assess potential "what if" scenarios and plan for the worst-case scenario can prevent or at least minimized the effects of system outages. Critical systems should be protected with some form of redundancy.
V23. NETWORK RESILIENCY VULNERABILITIES: CONTRACT MANAGEMENT
Maintenance contracts must be managed and maintained in order to avoid unsupported hardware and software.
V24. NETWORK MONITORING
When problems take place intermittently or only at peak times, they may be difficult to identify at the time. However, when ongoing network monitoring is in place, you can follow logs like a roadmap to recognize key trends in performance and network health.
V25. NETWORK LOGGING & AUDITING VULNERABILITIES: AUTOMATED LOGGING AND REPORTING
All critical systems should have automated logging and other reporting mechanisms in place in order to provide proactive analysis's to support system investigations and audits.
V26. NETWORK LOGGING & AUDITING VULNERABILITIES: SCHEDULED REVIEWS
Logs need to be reviewed on a regular basis as part of an overarching security program.
V27. IDENTIFICATION AND AUTHENTICATION VULNERABILITIES: ACCESS CONTROL
Access control and permissions need to be reviewed on a scheduled basis.
V28. IDENTIFICATION AND AUTHENTICATION VULNERABILITIES: SYSTEMS ACCOUNT REVIEWS
Systems need to be reviewed on a regular basis in order to identify unauthorized accounts.
V29. BUSINESS CONTINUITY AND DISASTER RECOVERY VULNERABILITIES: BACKUP
Systems are not backed up in a manner or frequency appropriate to the system criticality and type of data.
V30. BUSINESS CONTINUITY AND DISASTER RECOVERY VULNERABILITIES: PLANNING
There are no formal BCP or DRP plans in place to ensure the organization has sound recovery and continuity processes.
V31. BUSINESS CONTINUITY AND DISASTER RECOVERY VULNERABILITIES: ASSET INVENTORY
IT asset inventories are required for all computers and network devices considered to be "in-scope" for the BCP or DRP
V32. BUSINESS CONTINUITY AND DISASTER RECOVERY VULNERABILITIES: TESTING
BCP/DRP plans need to be tested at least annually.
V33. DATA CENTRE FACILITY VULNERABILITIES: FIRE SUPRESSION
Inadequate fire suppression is in place within a data centre hosting IT assets.
V34. DATA CENTRE FACILITY VULNERABILITIES: POWER AND COOLING
Inadequate power and/or cooling is in place within a data centre hosting IT assets.
V35. DATA CENTRE FACILITY VULNERABILITIES: WATER DAMAGE
A data centre hosting corporate IT assets has deficiencies that may cause flooding or other types of general water leakage that could damage IT assets.

VULNERABILITY CODES
V36. RESOURCE VULNERABILITIES: LOSS OF STAFF
The IT team may have the risk of losing key staff that would result in a fundamental gap in system/infrastructure knowledge.
V37. RESOURCE VULNERABILITIES: CROSS-TRAINING
There are no or limited cross-training processes in place that have exposed gaps in the support of critical IT systems. For example: if a single individual were to leave the organization or be absent to a period of time, a system outage could have serious adverse effects on the delivery of IT services.
V38. CLOUD VULNERABILITIES: USER PROVISIONING
a) Customer cannot control provisioning process, b) Identity of customer is not adequately verified at registration, c) Delays in synchronization between cloud system components(time wise and of profile content) happen, d) Multiple, un-synchronized copies of identity data are made, e) Credentials are vulnerable to interception and replay. .
V39. CLOUD VULNERABILITIES: HYPERVISOR VULNERABILITIES
Hypervisor-layer attacks are very attractive: the hypervisor in fact fully controls the physical resources and the VMs running on top of it, so any vulnerability in this layer is extremely critical. Exploiting the hypervisor potentially means exploiting every VM. A typical scenario enabled by exploiting a hypervisor's vulnerability is the so called 'guest to host escape', an example of which is 'VM hopping': in which an attacker hacks a VM using some standard method and then – exploiting some hypervisor vulnerability – takes control of other VMs running on the same hypervisor.
V40. CLOUD VULNERABILITIES: POOR KEY MANAGEMENT PROCEDURES
Cloud computing infrastructures require the management and storage of many different kinds of keys; examples include session keys to protect data in transit (e.g., SSL keys), file encryption keys, key pairs identifying cloud providers, key pairs identifying customers, authorization tokens and revocation certificates. Because virtual machines do not have a fixed hardware infrastructure and cloud based content tends to be geographically distributed, it is more difficult to apply standard controls, such as hardware security module (HSM) storage, to keys on cloud infrastructures.
V41. CLOUD VULNERABILITIES: LACK OF SECURITY AWARENESS
Cloud customers are not aware of the risks they could face when migrating into the cloud, particularly those risks that are generated from cloud specific threats, ie, loss of control, vendor lock-in, exhausted CP resources, etc. This lack of awareness could also affect the cloud provider who may not be aware of the actions that should be taken to mitigate these risks.
V42. CLOUD VULNERABILITIES: INADEQUATE PHYSICAL SECURITY PROCEDURES
These can include: a) lack of physical perimeter controls (smart card authentication at entry), b) lack of electromagnetic shielding for critical assets vulnerable to eavesdropping.
V43. CLOUD VULNERABILITIES: LACK OF RESOURCE ISOLATION
Resource use by one customer can affect resource use by another customer. IaaS cloud computing infrastructures mostly rely on architectural designs where physical resources are shared by multiple virtual machines and therefore multiple customers. Vulnerabilities in the hypervisor security model may lead to unauthorized access to these shared resources. For example, virtual machines of Customer 1 and Customer 2 have their virtual hard drives saved in the same shared LUN (Logical Unit Number) inside a SAN. Customer 2 may be able to map the virtual hard drive of Customer 1 to its virtual machine and see and use the data inside it.
V44. CLOUD VULNERABILITIES: USER DEPROVISIONING
Deprovisioned credentials are still valid due to time delays in roll-out of revocation.
V45. CLOUD VULNERABILITIES: LACK OF OR WEAK ENCRYPTION OF ARCHIVES AND DATA IN TRANSIT
Failure to encrypt data in transit, data held in archives and databases, un-mounted virtual machine images, forensic images and data, sensitive logs and other data at rest puts the data at risk. Of course the costs of implementing key management [V11] and processing costs must be taking account and set against the business risk introduce
V46. CLOUD VULNERABILITIES: DATA PORTABILITY
The organization needs to have the ability to "move" corporate applications/data between on-premise and cloud services from different providers.
V47. CLOUD VULNERABILITIES: INTEROPERABILITY
Public and private cloud services need to understand each other's APIs, configuration, data formats and forms of authentication and authorization. Interfaces are standardized, so that the organization can switch from one cloud service to another with minimal impact to enterprise systems.
V48. CLOUD VULNERABILITIES: VENDOR LOCK-IN
Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one cloud provider to another. The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered due to factors such as non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.

VULNERABILITY CODES
V49. CLOUD VULNERABILITIES: PROVIDER DUE DILIGENCE
Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.
V50. CLOUD VULNERABILITIES: CORPORATE CLOUD POLICY
A corporate policy on cloud usage may not exist or be inadequate (e.g. out-dated). A policy provides guidelines for secure and effective cloud computing operations to ensure the integrity and privacy of company-owned information.

Appendix E – Cloud Applications

REPORT CARD

CLOUD SERVICE CATALOGUE

Cloud Service Catalogue	Tier 1 (0-4 hours)	Tier 2 (24-hours)	Tier 3 (3-days)	Tier 4 (7-days)
AEDInspections(FindMyAED)				
AmbulanceAVL(FleetCenter)				
AmbulanceDispatch(FatPot)				
AssetAuction(GovDeals)				
BedTransfers(PTAC)				
BiddingandRFPAssessment(Bonfire)				
CapitalAssetPlanning(CityWide)				
Communication(Skype)				
CommunityParamedic(DocMeIn)				
CorporateStrategy(Envisio)				
DaycareProvidorDiscovery(ONEHSN)				
DeathRecords(ServiceOntarioFormsPortal)				
Design(Canva)				
DigitalAssetManagement(ThirdLight)				
DrugInformationService(Pepid)				
ElectronicHealthRecords(eConnect)				
EmergencyVolunteerManagement(SAVE)				
EMSDocumentManagement(iMedic)				
EnergyReporting(LASReportingTool)				
ePayments(Stripe)				
FinancialManagement(BDOClientPortal)				
FoodOrdering(SyscoPortal)				
FoodService(SyscoSynergy)				
GIS(ESRI)				
HealthRecords(eConnect)				
HospitalTraining(BaseHospitalTraining)				

ICON2.0(French Trial Notices)				
Invoicing(Quickbooks)				
LTCManagement(OurTeam)				
LTCResidentTestResults(LifeLabs)				
MaintenanceIssueTracking(WorxHub)				
MandatoryReporting(LTCHomesDotNetPortal)				
MuseumDonations(DonorBox)				
NursingSkillsAssessment(AIS)				
NursingSupplyOrders(MedicalMart)				
OnlineBanking(TD)				
ParamedicDataService(EasyView)				
PatientHealth(PointClickCare)				
PharmacyForms(ClassicCare)				
PropertyManagement(Yardi)				
RecreationPlanning(ActivityPro)				
RemotePatientMonitoring(IdealLife)				
ResidentWaitingListandApproval(CCACPortal)				
RideCoordination(TripSpark)				
RoadCompliance(Oscar)				
RoadConditions(Wood)				
Scheduling(StaffScheduleCare)				
ServiceCanada(RecordofEmployment)				
ShiftFilling(StaffStat)				
SituationalAwareness(Responder511)				
SMSMaintenanceSSClients(Connect)				
SocialAssistanceManagement(SAMS)				
TaxAndAssessmentResearch(MPAC)				
TicketSales(EventBright)				
Training(Relias)				
Training(SurgeLearning)				
VolunteerManagement(Volgistics)				
WSIBClaims(Ontario.ca)				