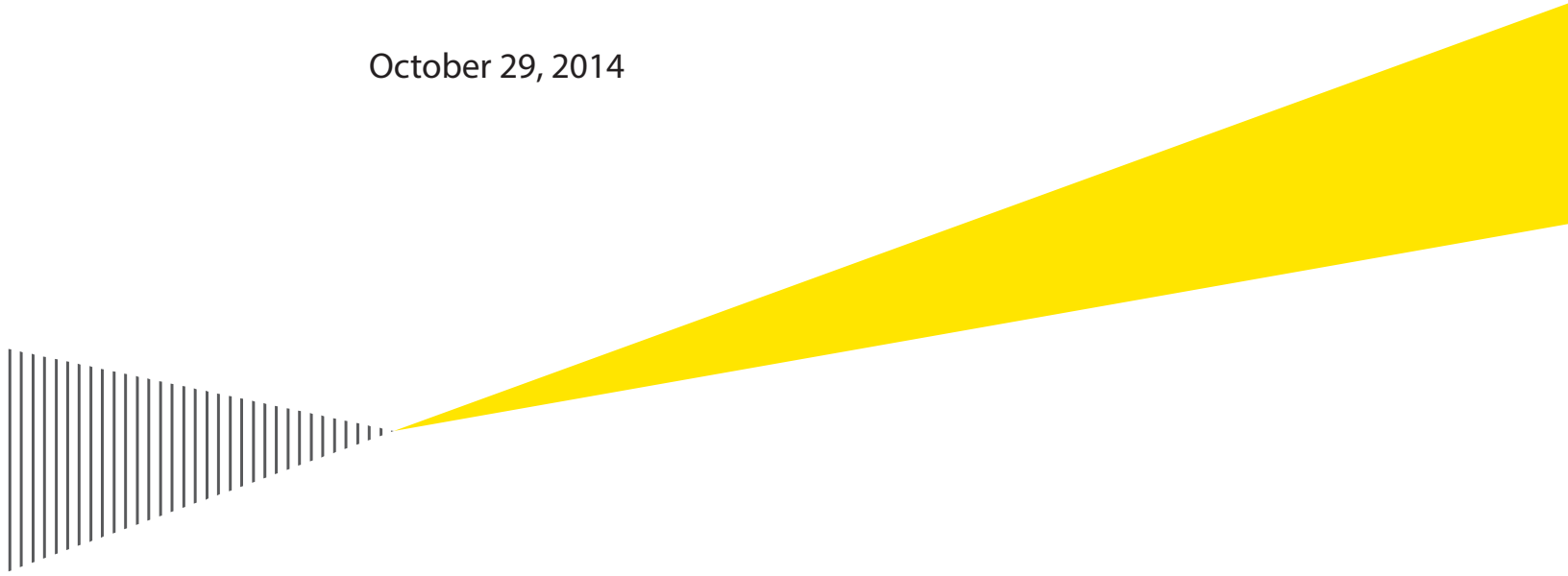
Marysville Data Centre Incident Review

Final Report

October 29, 2014

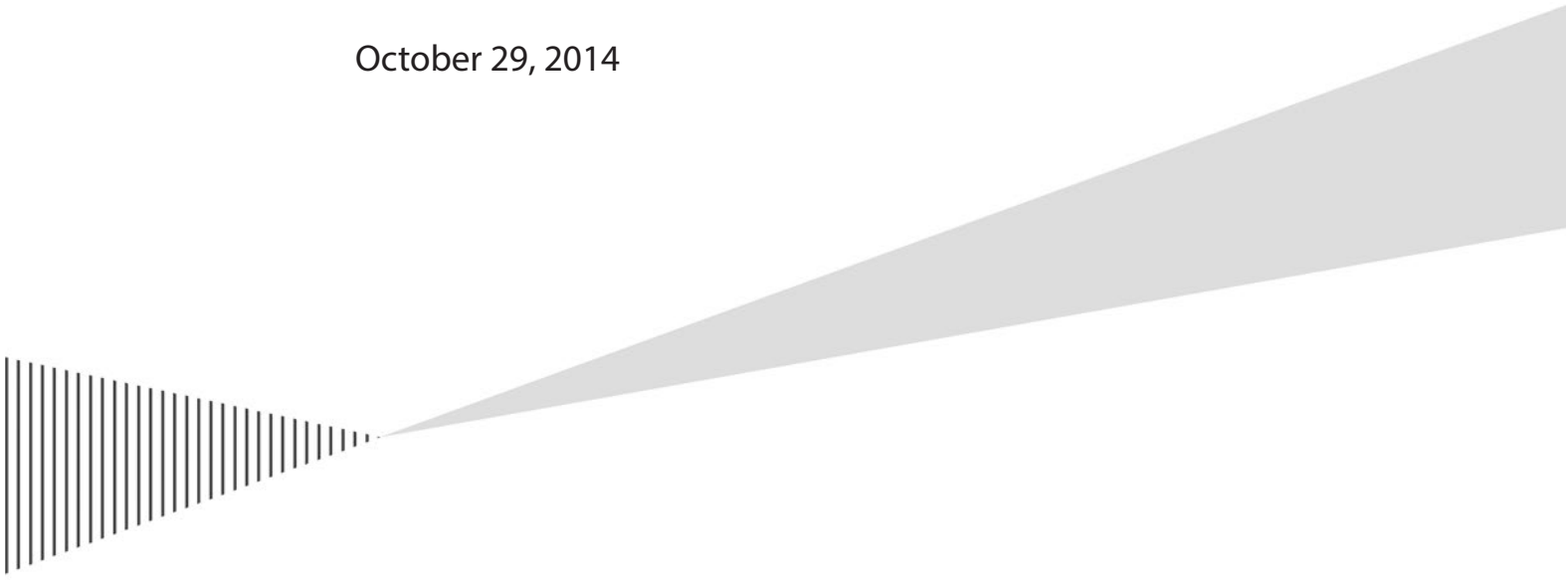


Building a better working world

Marysville Data Centre Incident Review

Final Report

October 29, 2014



EY

Building a better working world

Marysville Data Centre Incident Review
Final Report

Prepared For:
Government of New Brunswick

Prepared by:
Ernst & Young LLP

October 29, 2014

10040

Table of Contents

1 Executive Summary

Over the past six weeks Ernst and Young (EY) has conducted an investigation of the data centre services outages that occurred in June of this year. The investigation has focused on gaining an accurate understanding of the chronology of events that were triggered by the initial electrical outage impacting the Marysville data centre on June 9th, subsequently determining the root causes of the related data centre services outages. Additionally, a high level business impact assessment has been completed to determine an order of magnitude understanding of the financial and business operations impacts arising from the loss of services to Government of New Brunswick (GNB) business operations.

Several key findings have resulted from these investigations, along with related recommendations for the Government of New Brunswick. Recommendations have been developed providing immediate, actionable measures to mitigate the risk of future service outages, also identifying opportunities for GNB to improve data centre service delivery and reduce their respective costs.

A combination of methods were utilized, i.e. group workshops, individual interviews and documentation reviews involving relevant stakeholders, both internal and external to GNB, to provide a comprehensive accounting of the chronology of events associated with the Marysville data centre outages, capturing key event activities, technology issues, decisions points and leadership involvement in incident recovery.

The findings identified that the initial electrical services interruption to the facility led to a cascading series of other key facilities infrastructure failures resulting in several full data centre services outages at the Marysville facility. Following the initial electrical service interruption, the electrical system Automatic Transfer Switch (ATS), Uninterruptable Power Supply unit (UPS), on-site standby generator and the subsequently procured temporary portable generator all failed; a "perfect storm" of coincidental equipment failures. Investigations revealed that relevant facilities infrastructure equipment was being maintained in accordance with generally accepted manufacturers recommendations and industry practices; however the age and degree of use of certain equipment components may have been contributing factors to the failures. The current design of the data centre supporting facilities infrastructure does not provide for component redundancy, i.e. no dual incoming utility electrical service, single ATS, single UPS, and single on-site standby generator.

It was determined that the response measures and decisions taken during the incident to address the multiple equipment failures were appropriate. Given the situation and circumstances, overall, the incident recovery activities were generally well managed and key decisions taken were appropriate.

To identify key business impacts resulting from the outages, EY developed a Business Impact Assessment Survey to be completed by New Brunswick Internal Services Agency's (NBISA) client organizations. Most departments identified loss of productivity as the principal impact of the outages. Many departments also identified data loss and data corruption as significant issues resulting from the outages. This contributed to the length of time clients did not have access to some of the files required to perform their essential functions. Information gathered from NBISA client organizations indicated there were varying levels of external impact to the public, with most impacts being limited in duration; no public safety, property or life-threatening impacts were reported. Loss of revenue to GNB was reported as not significant, as only a few client organizations generate revenue, and potentially, revenue that was not generated during the outages may have been deferred, not lost. From the information gathered, our overall assessment of the impact to GNB business operations is that the service outage impacts were serious but of limited duration, with cost implications, to the degree they could be determined, of approximately $1.6M, including investment in replacement equipment. The loss of productivity was quantified using input from various client organizations and estimated at a value of approximately half a million dollars with NBISA and client organization direct remediation and recovery costs of approximately $1.1M.

Key findings and recommendations to mitigate the probability of future service outages include:

- Improving applicable governing processes in major IT service outage situations;
- Integrating these processes with broader crisis management practices of GNB;
- Reviewing and improving facilities infrastructure maintenance and testing procedures;
- Implementing secondary, portable generator capabilities for the Marysville and
  ;
- Fixing network routing/failover issues the NBISA data centres; and,
- Assessing other aged infrastructure components at the Marysville data centre for potential future upgrade to further mitigate business interruption risk.

Additional longer term recommendations relate to the current data centre facilities architecture and operational management model. This recent incident brings to light several issues with how GNB currently delivers data centre services and opportunities to provide them more cost effectively in the future.

1. One of the most critical findings is that GNB does not have an accurate inventory of applications that are supported in the NBISA data centres and there exists no accurate mapping to supporting infrastructure. With this situation and with the current management model for data centre services, i.e. distributed, GNB may not be designing and implementing technology infrastructure in the most cost effective manner, nor in alignment with the availability requirements of client organization applications. We recommend that a complete inventory of applications and supporting infrastructures be developed.
2. GNB does not have an established disaster recovery site for recovering critical GNB IT services/ systems in the event that services are interrupted for a long duration; it is strongly recommended that GNB assess the need for this capability and implement accordingly.
3. Significant cost savings, service performance and reliability improvement opportunities exist for GNB through approaching the provision of data centre services from a more holistic perspective, developing a data centre facilities strategy that takes advantage of recent advances in server and storage technologies, technology consolidation and resulting facilities rationalization opportunities. Through the development and implementation of a comprehensive GNB data centre facilities and services management strategy that addresses governance, technology optimization opportunities, and facilities and operational management, GNB could provide improved IT services performance and reliability to its clients and reduce the long-term costs associated with providing data centre services.

2 Project Overview

2.1 Background

NBISA is accountable for management of the Marysville Place data centre. This data centre is managed through a Master Services Agreement (MSA) with Bell Aliant. Departments and agencies subscribe directly for the service needed to support their program delivery from the standard services defined through the MSA. Activities associated with daily operations, and management of the data centre and services are the responsibility of Bell Aliant. The facilities and facilities infrastructure supporting the data centre are the responsibility of and are managed through the Facilities Management Branch of the Department of Transportation and Infrastructure (DTI).

Marysville data centre experienced a power outage on 9 June 2014, which caused a series of events resulting in complete shutdown of the data centre. This critical incident has caused a perceived significant business impact to NBISA and its clients. NBISA has engaged EY to evaluate the incident and to perform a comprehensive incident review.

EY has worked with NBISA and other key stake holders to perform an analysis of this critical incident and related or subsequent "child" incidents. As part of this process, EY has conducted a series of interviews with key stakeholders from NBISA, Bell Aliant, DTI, NB Power and Cummins, gathering and analyzing documentation related to the incident and recovery operations.

This report provides a consolidated chronology of events as they happened during the critical incident, a Root Cause Analysis (RCA), a high-level business impact analysis and several key findings and recommendations.

2.2 Scope & Objectives

The engagement scope included assessment and analysis of the incident and documentation of its chronology, root causes and general business impacts.

The key objectives of this engagement are:

Review and create a consolidated version of the chronology of the incident	Perform analysis of the incident and identify root causes of the incident	Identify key business impacts, including order of magnitude costs, across affected Province of New Brunswick business operations	Develop a proposed "Roadmap for GNB", relevant to the Root Cause Analysis findings and recommendations
✓	✓	✓	✓

To achieve these objectives, EY:

- Developed an objective and independent RCA report
- Identified key data centre facilities technology and applications systems "Single Points of Failure" (SPF) and remediation recommendations
- Conducted a survey of impacted NBISA client organizations and follow-up interviews with client organizations to perform a general, high level Business Impact Analysis
- Highlighted leading practices in the market in the area of data centre incident management, and
- Developed recommendations for NBISA and the Government of New Brunswick (GNB).

2.3 Deliverables

Our deliverable, the final report, contains the following key sections,

- **Consolidated Incident chronology**:

  The timeline of events as it happened during the incident has been documented in this section. This section also includes a review of the incident response activities and key decisions taken during incident recovery.

- **Root Cause Analysis**:

  In this section EY analyzed the root causes of the main and child incidents.

- **Business Impact Analysis**:

  This section contains the review and assessment of key business impacts resulting from this incident to both NBISA and its clients. It also has the survey results and the key findings derived from them, including an "order of magnitude" incident cost estimate to GNB.

- **Industry leading practices related to this incident**:

  This section highlights some of the key leading practices followed by industry for handling and managing these types of critical incidents.

- **Key findings, recommendations and prioritized roadmap for NBISA**:

  Key findings and observations from the analysis and assessment performed during the course of this engagement are listed here. This section also highlights our key recommendations and a preliminary (requiring further GNB analysis), prioritized roadmap of recommended activities for NBISA and GNB.

2.4 Approach

EY's approach to this particular engagement was divided into three phases as detailed below:

Data Centre Incident Review

	Phase 1 **Project Kick-off & Information Gathering (3 Weeks)**	Phase 2 **Information Assessment & Analysis (3 Weeks)**	Phase 3 **Documentation & Report Submission (2 Weeks)**
EY Approach and Activities	Preliminary Planning and Approach Kick Off Comprehensive review of recent incident • Documentation Collection and Initial Review I.E.: Logs, Chronology, Reports and Summaries • Incident team and stakeholder Interviews • Facilities Site Visit • Data Centre Assessment – Incident-related Operations & Technology • Vendor Consultations • Collection of Incident Costs from business units • Impact Analysis and review of NB ISA DC supported core business functions for analysis relevant to IT Service Continuity Management (ITSCM) and disaster recovery	Information Assessment • Interview material review • Documentation detailed review and consolidation • Consolidated Incident Chronology development Data analysis Secondary interviews and follow up activities Correlation of incident costs Leading practices comparisons Final analysis and collation of all material RCA Preliminary Reporting & feedback	Activities related to preparation of final reports • Business Impact Analysis • Preparation of RCA Documentation/Report • Development of Recommendations Preliminary review with NBISA and GNB designates Final report development Final report submission and presentation as needed
GNB Contribution	Provide the project team with any required documentation Ensure the proper cooperation of process owners and other key stakeholders Review and approve the plan of action	Collaborate with the project team to ensure alignment on approach and activities Facilitate the scheduling of key events including interviews and presentations to stakeholder groups as appropriate	Timely review and agreement on the drafts of the report and engagement deliverables

3 Chronology of the Incident

3.1 Marysville Data Centre Design

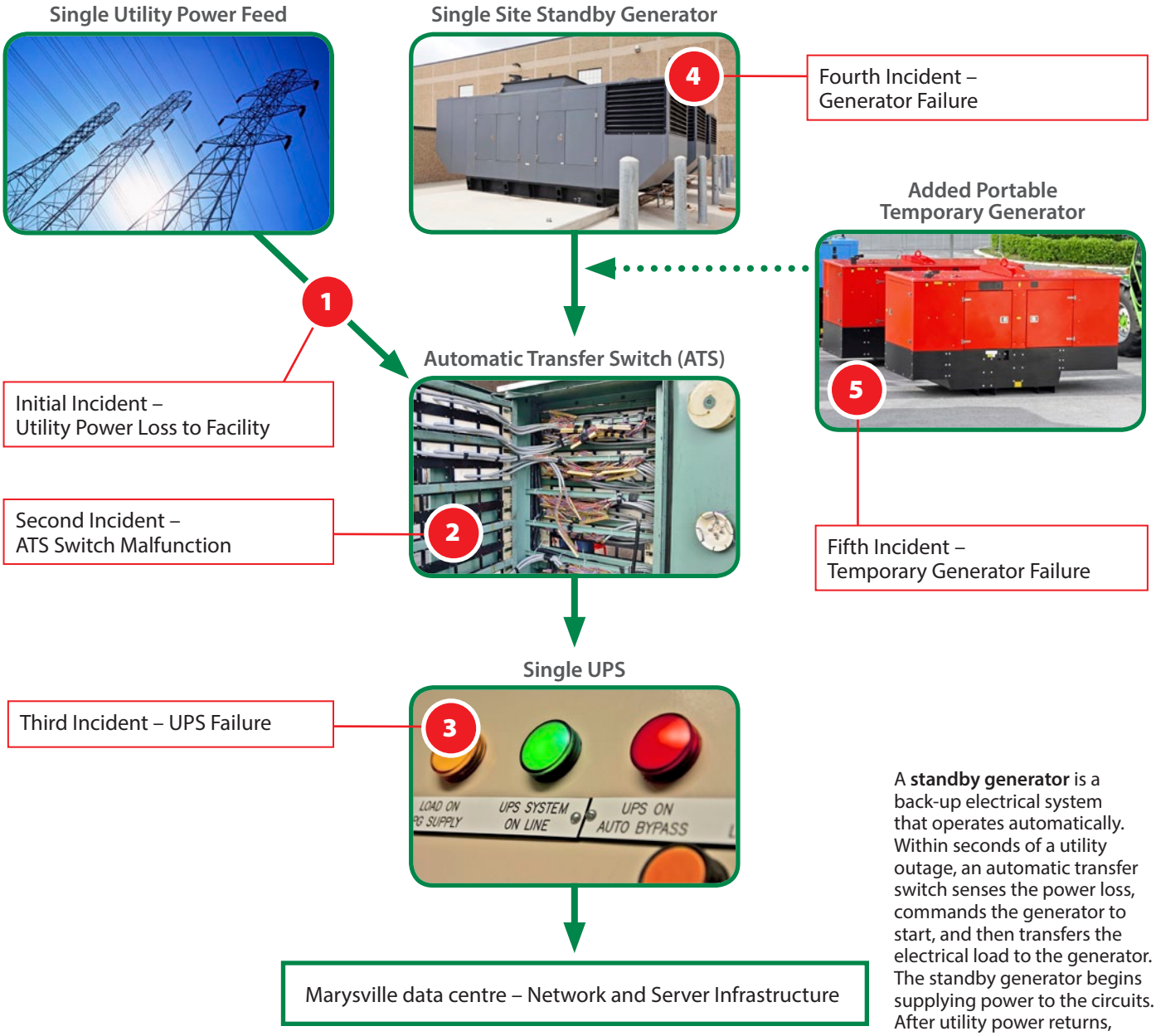
The GNB Marysville data centre has an electrical infrastructure design that provides for a single main electrical feed into the facility from the utility power provider. To condition the incoming power and to support facility systems for a short period of time (approximately 15 minutes), in the event of a utility power interruption, a single Uninterruptible Power Supply (UPS) is installed. In addition to the main utility power feed, and as a longer term backup power source in the event of power interruption, a single diesel generator supports the facility. For switching incoming power feeds to the UPS from the utility power to the generator fed power, or vice versa, an Automatic Transfer Switch (ATS) is incorporated into the electrical system design.

In the event of a utility power disruption, this electrical design should maintain the facility without incident or impact. This system is automated and under normal operations is meant to require no human interaction or intervention.

With a utility power outage, the UPS is designed to provide protection from input power interruptions by supplying energy to facility systems through battery stores within the UPS. Within seconds of a utility power outage, the Automatic Transfer Switch (ATS) is designed to sense the power loss, and commands the standby generator to start. The ATS will then transfer the electrical feed to the UPS to be from the generator, and the generator will then be supporting the electrical needs of the facility systems. After utility power returns, the automatic transfer switch is designed to transfer the electrical load back to the utility power feed and signals the standby generator to shut off. It then returns to standby mode where it awaits the next outage.

3.2 Incident Depiction

The diagram below provides a pictorial overview of the key data centre facilities infrastructure impacted during the series of outages that occurred.



An **Automatic Transfer Switch (ATS)** is often installed where a standby generator is located, so that the generator may provide temporary electrical power if the utility source fails. This switch acts as an interconnection between the various power sources in a redundant power system. It is deemed to be a critical component at the Marysville data centre.

An **Uninterruptible Power Supply** (**UPS**) is an electrical device that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries. The on-battery runtime of most uninterruptible power sources is relatively short (only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment. The UPS also provides a power conditioning feature that normalizes the power to the various systems and protects from surges, spikes and variation in operating frequencies.

A **standby generator** is a back-up electrical system that operates automatically. Within seconds of a utility outage, an automatic transfer switch senses the power loss, commands the generator to start, and then transfers the electrical load to the generator. The standby generator begins supplying power to the circuits. After utility power returns, the automatic transfer switch transfers the electrical load back to the utility and signals the standby generator to shut off. It then returns to standby mode, where it awaits the next outage.

Portable Generator
Similar to a Standby Generator but able to be transported and placed at a remote site. Typically a rental or temporary secondary devices.

3.3 Incident Timeline

GNB faced a critical incident at its Marysville data centre due to power outage followed by sequential failure of its Automatic Transfer Switch (ATS), Uninterrupted Power Supply (UPS) and Diesel Generator.

A consolidated Incident Log has been prepared to provide a detailing of the chronology of events that took place. Information has been gathered through a series of interviews with key vendors and stakeholders who were involved in this incident, and review of any available incident related documentation. As much of the evidence and info was collected verbally, best efforts have been made to maintain continuity and objective recording of the events timeline.

Consolidated Incident Log	
Date Time (Approx.)	**Activity Performed**
9 June 2014	
9.15	Utility power fails for approximately 2.5 seconds.
9.15	Utility power is restored, but fails shortly after. Outage lasts for approximately 29 minutes.
9.15	The ATS fails to switch the input power source to the standby generator (750 KW). The UPS continues to carry the load. No alerting of the ATS malfunction was noted at the annunciator panel located on the data centre floor. UPS technician notifies the on-site team of the ATS malfunction. UPS technician informed the Bell Aliant team that there was approximately 10 minutes of capacity on the battery reserves.
9.30	As a precaution, on-site technicians proceeded to shut down the Mainframe with the UPS back-up still taking load.
9.35	UPS battery plant is depleted and the UPS shuts down causing a full shut down of the data centre infrastructure.
9.40	from Bell Aliant immediately communicated the situation to from NBISA.
9.44	Utility power is restored and fails shortly afterward. It is restored again at 10:10. There were some issues with UPS and progressive troubleshooting revealed that the fuses had "blown". This was potentially due to the power surge at the onset of restored utility power. It took 5 hours to procure the required fuses for the UPS from Halifax.
10.30	After a situational assessment including an emergency meeting, the ATS is placed in back-up mode and locked out (cannot transfer back to utility power), the breakers are set to bypass the UPS, and power is restored to the data centre from the diesel generator.

Consolidated Incident Log	
Date Time (Approx.)	**Activity Performed**
11.39	There is a partial interruption in power (fluctuations) to the data centre attributed to trouble-shooting of the ATS by the Cummins technician. Power is immediately restored to the floor. Mainframe is still down at this point. Various other systems that were being restored at the time were impacted and may have incurred a hard shut down.
13.45	As the IT services/devices in the data centre are restored, the electrical load on the generator increases. By 13:45 the diesel generator is unable to provide sufficiently stable power to the data centre. The generator begins to falter and subsequently shuts down. The on-site Cummins technician identified that there was an issue in the provision of fuel to the generator (crack in pre-filter) and that the generator failure was not due to an inability of the generator to provide the required power to meet the demanded requirements to the facility, refuting an earlier assumption.
14.00	The decision is executed to shut down all power to the data centre since the generator failed. The on-site team was not comfortable using the utility power at this stage. Utility power was being used to power the lights/safety in the facility, but not the data centre. Up until this point in time, decision making was made by NBISA with the input of DTI and Bell Aliant technical staff.
	took over decision-making leadership at this point for NBISA. Up to this time, communication had generally been between Bell Aliant representatives in contact with NBISA resources; this was the first formalization of an incident command structure.
	GNB Clients were updated by NBISA about the current incident through conference calls. NBISA was being updated by Bell Aliant through technical team conference calls.
14:45	Replacement fuses for the UPS arrive on-site. Upon replacement the system indicated that the DC regulator board had failed in the UPS. During subsequent testing, a physical failure occurred in the primary switch, which is believed to have allowed 600+ volts to cross the low voltage circuitry. Repair efforts subsequently began, focusing on sourcing of required parts.
16.00	Decision was made by NBISA to restore power to the data centre from the utility source. This source was unconditioned due to the previous failure of the UPS.
	Network connectivity was available at this point and the on-site technical team was ready to restart the affected IT systems. It took approximately an hour to bring the systems back and into production.
17.00 : 22.00	DTI was able to source a 500KW portable generator from a regional source and the logistics of having it delivered to site were completed.
22.00	A 500KW portable diesel generator arrived on-site and at 22:00 the data centre took an emergency outage and the shutdown of all operational IT systems and building operations was completed to allow for the connection of the temporary generator.
23.30	Power is restored to the data centre from the 500KW portable diesel generator and ATS was manually locked out in the generator mode.

Consolidated Incident Log	
Date Time (Approx.)	**Activity Performed**
	Bell Aliant was working with NBISA to bring the SAN (Storage Area Network) back up and they were facing some data corruption issues.
10 June 2014	
2.00	IT systems were brought back up by 2 a.m. The Exchange Email system was operational shortly thereafter.
11 June 2014	
	Bell Aliant brought in engineering and operations team to perform a detailed analysis of the incident.
13 June 2014	
	communicated that he has been assigned the responsibility as prime for this incident from DTI.
	Electric Fuel Controller was changed in the standby generator.
15 June 2014	
7.00	A planned outage is taken to perform oil and filter change on the 500KW portable diesel generator. The data centre is de-energized at 7:00 and re-energized at 14:35. The data centre is once again powered by the 500KW temporary portable diesel generator.
	The incident response team tried replacing the electronic control device in the 750KW standby generator, but it did not resolve the problems it had been experiencing. It failed again under load test, requiring continued use of the portable generator. However, it was discovered that the 750KW standby generator system worked properly when the pre-filter was removed.
	Decision was made to move back to the main facility 750KW standby generator during the next service scheduled for June 22nd.
	Decision was made that Bell Aliant was to order a new ATS.
16 – 19 June 2014	
	A separate, temporary, stable and essential power stream has been established to allow the removal of the malfunctioning equipment and the installation of new permanent equipment in the same physical location. This temporary power stream also included the migration of the data centre air conditioning circuits onto a temporary power panel so that maintenance could be carried out on the data centre's substation during the upcoming outage planned for June 22nd ..
18 June 2014	
	Temporary rental ATS arrives on-site.
20 June 2014	
7.00	500KW portable generator was fueled under load.
7.20	The 500KW portable diesel generator fails due to a clogged fuel filter and a full outage is taken by the data centre.

Consolidated Incident Log	
Date Time (Approx.)	**Activity Performed**
7.45	Power is restored to the data centre with utility power. This switching of power feeds is done without any approvals.
8.10	Corporate IT services are restored.
22.00	Another similar sized, 500KW, portable diesel generator was brought on-site and an outage was planned to switch over to the new generator. At 22:00 the data centre took an emergency outage to switch to the diesel generator. The switch was completed at 23:30.
21 June 2014	
	During the testing of the temporary ATS, the new additional 500KW portable diesel generator and portable 500KVA UPS, it was realized that the generator did not have the capacity to power the temporary UPS and that a larger generator would be required. The size of the facility diesel generator was adequate however there was lack of confidence in its condition. A 1MW portable diesel generator was sourced and brought on-site the same day. The 1 MW portable diesel generator arrived and was connected to the power stream, however during the testing with the ATS, the generator would not respond to the ATS's request to transfer so the automatic transfer option was not available. Technicians were not able to fix this and a decision was made with NBISA's input to use the facility diesel generator in the temporary power stream.
22 June 2014	
7.00	The data centre is powered down for a cut-over to the temporary power stream. The temporary power stream includes all infrastructure elements of the permanent power stream but with rented/leased components (ATS, UPS, and generator). Maintenance was carried out on breakers within the data centre substation during the shutdown.
17.00	Power is restored to the data centre with the temporary power stream in place and operational.
24 June 2014	
	Legacy UPS and ATS were decommissioned and disposed with no root cause investigation for the failures being conducted. The decision to remove the old UPS was made based on the advice of technicians and SME's, allowing the technicians to proceed with the installation of the new UPS. It has been indicated that retaining the old UPS would have resulted in delays, and the opinion of DTI was that the condition of the old UPS would have made it unlikely to draw any clear conclusions regarding the root cause of the problem.
17 August 2014	
07.00	The data centre is powered down for a cut-over to the permanent power stream.
11.30	Power is restored to the data centre with the permanent power stream in place and operational.

3.4 Key Findings Regarding Incident Response

The following table includes observations regarding what worked well (**green checkmarks**) and what could have been improved (**red x's**)

Key Findings on Response Activities

General:

- ✓ Despite the lack of a formalized and defined Major Incident Management process, nor a formal Emergency IT Change Management process, the response measures and decisions taken during the incident to address the multiple equipment failures were appropriate. Overall, given the situation and circumstances, the incident was generally well managed.

People:

- ✓ In general, the various participants in the response, including third party vendors and GNB technical and management staff, acted responsibly, collaboratively, and within the scope of their expertise.
- ✓ In the absence of defined process, the response team quickly established a command team and decision-making and communications structure to be applied during the incident.
- ✓ Personnel were particularly resourceful in sourcing and acquiring replacement equipment in an expeditious manner, e.g. second generator.
- × Roles and responsibilities of the various groups and individuals as applicable for a major data centre incident of this nature had not been clearly defined, either within an overall Major Incident Management process or as specific to data centre operations.
- × Actions were taken by on-site personnel without structured communication and documented change process approvals due to the initial absence of a proper Major Incident Manager or associated command team.
- × At least one vendor technician identified a lack of adequate training in the equipment he/she was supporting.

Process, coordination and communications:

- ✓ Once the severity of the incident was identified, a command centre was quickly established for centralized communication and collaborative decision-making.
- ✓ Key decisions were based on consensus and seemed appropriate based on the circumstances of the situation and available information that was known at the time.
- ✓ There were at least two NBISA client conference calls each day to provide an update to key stakeholder groups.
- ✓ The Service Desk was kept informed of the situation regularly in order to handle queries from clients.
- ✓ Bell Aliant, who maintains a Major Incident Management process, notified key vendors and stakeholders immediately upon identification of the outage.
- × There is no formalized Major Incident Management process within NBISA.
- × A communication plan with clearly identified communication channels (an integral aspect of any Major Incident Management process) had not been established and needed to be improvised or developed on an ad-hoc basis. As a result, ownership of communications was not initially clear within NBISA, their third-party vendors and clients (i.e. it was unclear who should lead engagement with NB Power (DTI ultimately took ownership)).

- ✗ There is no IT Emergency Change Management process or procedures.
- ✗ Restoration of the electrical system followed the protocols for a commercial facility without clear differentiation of the requirements for a data centre.
- ✗ No formal process exists to support emergency procurement and related funding appropriation and approvals.

Technology:

- ✓ Maintenance contracts were in place for all relevant equipment and third party vendor technicians responded quickly and within SLA's to the incident.
- ✗ The annunciator panel located on the data centre floor as well as the ATS console, showed no alarms or notification of ATS failure.
- ✗ Sourcing options for emergency replacement of failed equipment had not been identified, confirmed and defined in advance of the incident and needed to be researched during the incident.
- ✗ Contract governance related to the testing of fuel was not in place and potentially contributed to the performance failure of the on-site standby generator and the third-party temporary generator.

Governance:

- ✗ For a significant IT issue of this magnitude, there is no evident linkage available to NBISA into a broader GNB crisis management plan for loss of IT services– typically, the Major Incident Management process integrates into a broader crisis management plan.
- ✗ NBISA does not have a Disaster Recovery Plan for the data centre and hence had no option for restoring service other than to resolve the problems at the Marysville data centre.
- ✗ NBISA has an understanding of the systems and services for which they are directly responsible, but they do not have a clear understanding of the criticality of the systems hosted in the data centre or the system recovery priorities during an event of this nature.

4 Root Cause Analysis

4.1 Introduction

This Root Cause Analysis is based on interviews with key individuals and stakeholders involved in the incident. Much of the information and evidence provided was verbal in nature. There were some variances in accounts of the relevant events; within the limitations of this review, every attempt was made to confirm information received, however some assumptions were made based on analysis of the information received. Relevant documentation was provided and used to substantiate various claims and details; where applicable, they have been identified in the document.

NBISA faced a critical incident at its Marysville data centre due to a power outage, followed by sequential failure of its Automatic transfer Switch (ATS), Uninterrupted Power Supply (UPS) and Diesel Generator. This Root Cause Analysis is prepared with information gathered from vendors and key stakeholders who in the incident.

The incidents have been broken down into seven separate events, with the primary event being referred to as the "Parent Incident" and all subsequent incidents being referred to as "Child Incidents".

4.2 Stakeholders Interviewed

List of People Interviewed		
Name	**Team**	**Date**
	Deputy Minister (DGS)	4-Sep-14
	Vice President, Operations & former Acting VP, ITaaS (NBISA)	4-Sep-14
	Director, IT Operations & IT Service Desk (NBISA)	3-Sep-14 & 6-Oct-14
	Director, Business Strategy & Alignment (NBISA)	17-Sep-14
	Chief Technology Strategist (OCIO)	3-Sep-14
	Acting Director, IT Applications (NBISA)	3-Sep-14
	Manager, Client Relationship Management (DGS)	3-Sep-14
	Manager, IT Service Desk (NBISA)	3-Sep-14
	Manager, Network & Security Services (NBISA)	3-Sep-14
	Manager, IT Projects (NBISA)	3-Sep-14
	Supervisor, Facilities Management Fredericton Operations (DTI)	28-Aug-14
	Manager, Engineering Services (DTI)	28-Aug-14
	Account Executive (Bell Aliant)	4-Sep-14
	Enterprise Service Manager (Bell Aliant)	4-Sep-14
	data centre Site Manager (Bell Aliant)	4-Sep-14
	Engineering design for ATS & UPS (Bell Aliant)	4-Sep-14
	Engineering group (Bell Aliant)	4-Sep-14

List of People Interviewed		
Name	**Team**	**Date**
	Manager, data centre Facility (Bell Aliant)	4-Sep-14
	ATS Technician (Cummins)	12-Sep-14
	UPS Technician (Emerson)	25-Sep-14
	Distribution System Performance Engineer (NB Power)	20-Oct 14

4.3 Event Descriptions

4.3.1 Parent Incident: Utility Power Loss 9 June 2014

4.3.1.1 Summary of event

On 9th June 2014 at 9:15am AST there was a loss of utility power at the Marysville data centre. The initial loss was momentary; however, it failed again, resulting in a utility power outage for 29 minutes. During this time the UPS carried the load of the data centre IT systems, as designed.

The following chain of events resulted in the extended outage and instability of the systems and facility at the Marysville data centre.

Initial reports indicate that the electrical service outage was caused by an Osprey bird's nest that had fallen on the main power distribution lines to the area. Service was the responsibility of the vendor of record (NB Power).

Statement by NB Power was:

> "*Regarding the interruptions caused by osprey nesting*:
>
> *The interruptions of June 8th & 9th were due to an occupied osprey nest, two transmission line structures from the one above. Utilities are not allowed to remove an occupied nest. The nest was trimmed. The nest will be moved when annual nesting is finished.*"

4.3.1.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	9.15	Utility power fails for approximately 2.5 seconds.
	9.15	Utility power is restored, but fails shortly after. Outage lasts for approximately 29 minutes.

4.3.1.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
NB Power
Bell Aliant

- Review of incident details and logs
- Interview with site and incident personnel
- Review of provided documentation

4.3.1.4 Findings and Root Cause

- There is a history of power instability to the Marysville data centre
- Cause Identified: Utility Power outage that had no prior indication or means of avoidance by the NBISA stakeholders

4.3.1.5 Corrective Action

- None taken
- Power was restored by the utility provider
- Utility power is procured from NB Power and outside the control of NBISA

4.3.2 Child Incident 1: Automatic Transfer Switch (ATS) Malfunction/Failure

4.3.2.1 Summary of Event

At 9:15 a.m. AST the ATS did not function as designed and failed to transfer the power source from the utility source to the diesel generator. Under normal operations, upon the availability of the standby generator, ATS should have switched the building's power source to the available generator automatically.

With no on-site personnel qualified or trained in the manual operations of the ATS, the system could not be manually transferred to the alternate source. Action was delayed pending the arrival of the service technician.

The UPS system continued to carry load and maintain the data centre IT systems as designed until 9:35 a.m. when the battery system depleted and the UPS ceased functioning.

ATS Description: An Automatic Transfer Switch (ATS) is often installed where a standby generator is located, so that the generator may provide temporary electrical power if the utility source fails. This switch acts as an interconnection between the various power sources in a redundant power system. It is deemed to be a critical component at the Marysville data centre.

4.3.2.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	9.15	The ATS fails to switch the input power source to the standby generator (750 KW). The UPS continues to carry the load. No alerting of the ATS malfunction was noted at the annunciator panel located on the data centre floor. UPS technician notifies the on-site team of the ATS malfunction. UPS technician informed the Bell Aliant team that there was approximately 10 minutes of capacity on the battery reserves.
	9.30	As a precaution, on-site technicians proceeded to shut down the Mainframe with the UPS back-up still taking load.

4.3.2.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Bell Aliant

- Review of incident details and logs
- Interviews with site and incident personnel
- Review of provided documentation
- Visual inspection of the new hardware installed on-site

4.3.2.4 Findings and Root Cause

Investigation of the reason for failure of the ATS was limited due to the decision made not to perform a detailed analysis of the root cause for the failed hardware prior to its decommissioning and removal.

- It is presumed that the automatic component failed due to either mechanical factors or the failure of the electronic control system
- Potential contributing factors:
  - Age of system
  - Amount of cycles the unit had performed during its lifespan due to testing and power fluctuations
- Maintenance records were provided by the vendor of record and were reviewed to ensure compliance with maintenance requirements. Around 45 days prior to the actual incident, there was a failure and various key components were serviced and/or replaced
- The ATS worked as designed and expected during similar events over the last 30 days prior to the incident
- Interviews revealed a lack of training and local knowledge by the vendor of record for the ATS system. This is a contributing factor to the delay in resumption of the systems
- Cause attributed to mechanical failure of the ATS system

4.3.2.5 Corrective Actions Taken

- A new ATS was procured and installed and is currently in production. It has been tested and commissioned under the supervision of NBISA and DTI and/or its designate
- New monitoring and an attenuator panel have been installed on the data centre floor
- This installation has been confirmed as complete based on visual confirmation of EY team members and reports by on-site contractors

4.3.3 Child Incident 2: UPS Battery Depletion/Data Centre Full Outage

4.3.3.1 Summary

At 9:35am AST the Marysville data centre experienced a full power outage due to the depletion of the UPS battery systems. The UPS was functioning as designed at this time. The depletion of the battery bank was a direct result of failure of the ATS to transfer the power source to generator. Battery stores would not have been depleted had the ATS and generator system performed as designed.

All systems remained in an unpowered state until 9:44 a.m. AST when utility power was restored.

The UPS maintenance technician was on-site at the time of outage performing maintenance on the battery cells. The maintenance technician believed that this activity did not contribute in any way to the outage and may have aided in the investigation of the systems.

Maintenance records were provided by the vendor of record and were reviewed to ensure compliance with maintenance requirements.

*UPS Definition: An **Uninterruptible Power Supply** (**UPS**) is an electrical device that provides emergency power to a load when the input power source, typically main power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries. The on-battery runtime of most uninterruptible power sources is relatively short (only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment. The UPS also provides a power conditioning feature that normalizes the power to the various systems and protects form surges, spikes and variation in operating frequencies.*

4.3.3.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	9.35	UPS battery plant is depleted and the UPS shut down causing a full shut down of the data centre infrastructure.
	9.40	from Bell Aliant immediately communicated the situation to from NBISA.

4.3.3.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Bell Aliant
Cummins Diesel
Emerson (UPS vendor)

- Review of incident details and logs
- Interview with site and incident team personnel
- Review of provided documentation

4.3.3.4 Findings and Root Cause

- The power outage was found to have been caused by multiple contributing factors:
  - The utility power outage
  - The failure of the ATS to transfer to the generator system
  - The depletion of the battery stores on the UPS system due to failure of the ATS
- The UPS system performed as expected and designed
- Cause attributed to extended absence of available power source due to ATS system failure

4.3.3.5 Corrective Action

- Some critical systems were proactively shutdown to maintain data integrity. (i.e. Mainframe)
- No other actions were available in the absence of a viable power source
- A new UPS has been installed and commissioned. Bell Aliant, the site operations management team for the data centre, reports that four banks of batteries have been installed providing what is now estimated at roughly 60 minutes of back-up based on current data centre loads

4.3.4 Child Incident 3: UPS Failure

4.3.4.1 Summary of Events

Upon restoration of the utility power to the building an attempt to restart the UPS was performed. It was identified that fuses had failed and would need to be replaced. The fuses required were ordered and arrived on-site from Halifax approximately 5 hours after the incident.

Upon replacement of the fuses, a failure of the DC Regulator Board was identified, requiring further testing.

During testing and cycling of the main switch on the UPS, a failure occurred that allowed raw high voltage to reach the control system causing a catastrophic failure of the control system.

Required repair parts and procurement lead times were identified. During the sourcing of the parts it was decided on June 11th by NBISA, in conjunction with Bell Aliant, to procure and replace the UPS system.

During all of this activity battery back-up was non-functional. It is important to note that the facility was now operational on utility power.

4.3.4.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	9.44	Utility power is restored and fails shortly afterward. It is restored again at 10:10. UPS issues are experienced - progressive troubleshooting revealed that the fuses had "blown". This was potentially due to the power surge at the onset of restored utility power. It took 5 hours to procure the required fuses for the UPS from Halifax.
	10.30	After a situational assessment including an emergency meeting, the ATS is placed in back-up mode and locked out (cannot transfer back to utility power) and the breakers are set to bypass the UPS, and power is restored to the data centre from the diesel generator.

4.3.4.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Cummins Diesel
Emerson (UPS Contractor)

- Review of incident details and logs
- Interview with site and incident personnel
- Review of documentation provided
- Visual inspection of the new hardware installed on-site

4.3.4.4 Findings and Root Cause

Investigation of the failure of the UPS is limited due to the decision made not perform a detailed analysis of the failed hardware prior to decommissioning and removal.

- Liebert UPS device was documented as being 22 years old and was indicated by the support organization (Bell Aliant) that it had reached end of life. However, the manufacturer has confirmed that the official end of life for this device would not be reached until 25 years following installation
- In the vendor maintenance records it was noted that the UPS should be considered for replacement
- A Memorandum of Risk was issued on November 30th, 2011 by Bell Aliant and signed off on the 8th of December by NBISA indicating a heightened risk due to the age of the UPS system
- A Memorandum of Risk was filed again by Bell Aliant on 17 January 2012 that highlighted the concern associated with the UPS. In it, Bell Aliant is quoted as saying

"*A UPS failure will result in an interruption to all services provided by Bell Aliant.*"

- Based on vendor and support contract provider information, it is presumed that the system failed due to power fluctuations associated with the power outage and the failure of the ATS system
- Secondary failure and catastrophic failure of the main switch was attributed to the age of the switch
- Age of the device is considered to be a contributing factor. It has been indicated that the device had been in production for over 22 years
- While the device was under a maintenance agreement, no warranty existed and manufacturer parts support was based on "best effort"
- All maintenance was provided by Emerson, under contract from Bell Aliant
- Cause attributed to hardware failure; compounded by age of the system

4.3.4.5 Corrective Action

- The failed UPS was placed into a bypass mode to allow for unconditioned power to supply the facility
- Testing was conducted and further failure occurred
- The failed device was temporarily replaced with a temporary device on 22 June 2014 during the resumption efforts
- A new UPS has been procured and installed and is currently in production. This was commissioned and installed under the supervision of Bell Aliant, NBISA, DTI and/or its designates

4.3.5 Child Incident 4: Standby Generator Voltage Drop/Fluctuation

4.3.5.1 Summary of Events

The decision was made to run with the standby generator as the sole source of power to the facility to ensure continuity of service. The system was locked out to ensure it would remain on generator power until the decision to revert was made by the incident team.

At 11:39 a.m. AST the data centre experienced a power event and some systems were affected. This was due to actions taken by the ATS/Generator vendor attempting to lock the generator into a bypass run mode.

The incident was not a full outage, but a voltage and frequency fluctuation that affected some systems, and as such, impacted and delayed the resumption of services.

The power fluctuation impacted some systems that were being restored.

The generator was locked out and no further instances of the power fluctuation were noted.

4.3.5.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	11.39	There is a partial interruption in power (fluctuations) to the data centre attributed to trouble-shooting of the ATS by the Cummins technician. Power is immediately restored to the floor. Mainframe is still down at this point. Various other systems that were being restored at the time were impacted and may have incurred a hard shut down.

4.3.5.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Bell Aliant
Cummins Diesel

- Review of incident details and logs
- Interview with site and incident personnel
- Review of documentation provided

4.3.5.4 Findings and Root Cause

- System was set to the bypass generator only mode
- The system started a shutdown during the cycle of the switch
- The action by the vendor is deemed to have been correct and consistent with an attempt to secure the continuous running of the generator
- Cause attributed to unexpected reaction of the system to the change in switch state

4.3.5.5 Corrective Action

- Switch was locked out and generator source was secured

4.3.6 Child Incident 5: Primary Standby Diesel Standby Generator Failure

4.3.6.1 Summary of Event

On 9 June 2014, during the Marysville data centre power outage event, the on-site standby diesel generator failed to operate to specification and subsequently shutdown. This caused a full outage to the site. The systems were restored to unconditioned primary utility power. Investigation into the failure was completed and a secondary generator was brought on-site to support the data centre operations.

Further investigation identified failures in the fuel supply system and this was then remediated.

*Standby Generator Definition: A **standby generator** is a back-up electrical system that operates automatically. Within seconds of a utility outage an automatic transfer switch senses the power loss, commands the generator to start and then transfers the electrical load to the generator. The standby generator begins supplying power to the circuits. After utility power returns, the automatic transfer switch transfers the electrical load back to the utility and signals the standby generator to shut off. It then returns to standby mode where it awaits the next outage.*

4.3.6.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
9 June 2014	13.45	As the IT services/devices in the data centre are restored, the electrical load on the generator increases. By 13:45 the diesel generator is unable to provide sufficiently stable power to the data centre. The generator begins to falter and subsequently shuts down. The on-site Cummins technician identified that there was an issue in the provision of fuel to the generator (crack in pre-filter) and that the generator failure was not due to an inability of the generator to provide the required power to meet the demanded requirements to the facility refuting an earlier assumption.
	14.00	The decision is executed to shut down all power to the data centre since the generator failed. The on-site team was not comfortable using the utility power at this stage. Utility power was being used to power the lights/safety in the facility, but not the data centre. Up until this point, decision making was made by NBISA with the input of DTI and Bell Aliant technical staff.
	16.00	Decision was made by NBISA to restore power to the data centre from the utility source. This source was unconditioned due to the previous failure of the UPS.
		Network connectivity was available at this point and the on-site technical team was ready to restart the affected IT systems. It took approximately an hour to bring the systems back and into production.
	17.00 : 22.00	DTI was able to source a 500KW portable generator from a regional source and the logistics of having it delivered to site were completed.
	22.00	A 500KW portable diesel generator arrived on-site and at 22:00 the data centre took an emergency outage and the shutdown of all operational IT systems and building operations was completed to allow for the connection of the temporary generator.
	23.30	Power is restored to the data centre from the 500KW portable diesel generator and ATS was manually locked out in the generator mode.

4.3.6.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Bell Aliant
Cummins Diesel

- Review of incident details and logs
- Interview with site and incident personnel
- Review of documentation provided

4.3.6.4 Findings and Root Cause

Investigation of the failure of the Primary Standby Generator is limited due to the decision made not to perform a detailed analysis of the fuel filter. The filter was disposed of without analysis.

- The current 750KW standby generator is used to power both the general building systems as well as the data centre infrastructure
- There is no documented fuel testing procedure in place to minimize risk from contaminated fuel
- The initial investigation by the generator technician attributed the generator's "entering a frequency hunt state" due to a failure of the Electronic Fuel Controller (EFC) that regulates fuel flow to the generator. The suspected part was sourced by the vendor and ordered
- Upon installation of the part on the 15th of June it was identified that the frequency hunt condition was still present. Further investigation revealed a problem with one of the pre-filters that aids in the removal of particulate and contamination from the fuel supply. The seal was found to be broken and the filter bypassed.
- The 750KW standby generator was brought back into service; however a decision was taken to remain on the rental generator to ensure ongoing system continuity
- Cause attributed to a failure of the fuel flow filtering system that impacted the generator

4.3.6.5 Corrective Action

- Technician replaced the suspected Electronic Fuel Control (EFC) Module
- Technician bypassed the fuel system's pre-filter
- Standby generator was tested and readied to be put back into production
- A secondary generator was sourced and used as the primary power source for the facility

4.3.7 Child Incident 6: Secondary Diesel Generator Shut Down

4.3.7.1 Summary

Shortly after one of the scheduled refuelling of the rental/secondary generator, the unit malfunctioned and shut down. Technical teams were on hand and were able to intervene and bring the facility online with the use of utility power that had been deemed stable at that time.

A filter was identified as clogged and subsequently replaced.

4.3.7.2 Chronology of Events / Timeline

Date	Time (Approx.)	Activity Performed
20 June 2014	7.00	500KW portable generator was fueled under load.
	7.20	The 500KW portable diesel generator fails due to a clogged fuel filter and a full outage is taken by the data centre.
	7.45	Power is restored to the data centre with utility power. This switching of power feeds is done without any approvals.
	8.10	Corporate IT services are restored.
	22.00	Another similar sized, 500KW, portable diesel generator was brought on-site and an outage was planned to switch over to the new generator. At 22:00 the data centre took an emergency outage to switch to the diesel generator. The switch was completed at 23:30.

4.3.7.3 Investigative Team and Method

EY Team

Stakeholders

NBISA
DTI
Bell Aliant
Cummins Diesel

- Review of incident details and logs
- Interview with site and incident personnel
- Review of documentation provided

4.3.7.4 Findings and Root Cause

- The on-site technical teams attributed the failure to a clogged fuel filter on the Secondary Generator
- The unit had a full preventative maintenance completed on Sunday June 15th, where oil and all filters had been changed
- No information on the reason for the failure has been provided or determined and the discarded filter was not retained or sent away for any further testing or validation
- Fuel contamination is considered to be a possible cause of the filter failure
- Cause attributed to fuel filter contamination
- There is no documented fuel testing procedure in place to minimize risks associated with potentially contaminated fuel

4.3.7.5 Corrective Action

- The building was brought online with unconditioned utility power
- The filter was replaced in the generator that had the malfunction. However, given the uncertainty regarding the cause of the outage/issue at the time, the new generator brought on-site was used
- The facility was transferred back to generator power

5 Business Impact Analysis (BIA)

5.1 BIA Approach

EY was engaged to conduct a high-level assessment within a compressed timeline, identifying key GNB business operations impacts and determining "order of magnitude" cost impacts to GNB resulting from the data centre service outages. The full extent of external, i.e. citizen impacts, and potential reputational impacts to the Government of New Brunswick could not be determined through this analysis.

As the most effective method to quickly and within the parameters given identify key business impacts, EY developed a Business Impact Assessment (BIA) survey form to be completed by NBISA client organizations. The survey form consisted of several sections as described below:

A. Critical Services and Business Functions

The purpose of this section was to identify the critical (i.e. time sensitive) services and business functions performed by each department and the *potential* internal and external impacts if any of those services/functions could not be performed for an extended period of time.

B. Essential IT Systems

The purpose of this section was to identify the IT systems that are essential to each department's ability to deliver the services and functions identified in section A. Note that this included all IT systems, not just those hosted in the Marysville data centre.

C. Impact of Marysville data centre Outages

The purpose of this section was to identify the *actual* impacts, by client organization, of the Marysville data centre outages that began on Monday, June 9th, 2014, and to rank the severity of the impacts (i.e. high, moderate, low).

D. Financial Implications of Marysville data centre Outages

The purpose of this section was to identify the financial implications, by client organization, of the Marysville data centre outages. This included any lost revenue directly related to the outages, the internal cost of lost productivity, any extra costs incurred to recover from the outages, etc.

E. Other Implications of Marysville data centre Outages

The purpose of this section was to identify any other implications, by client organization, of the Marysville data centre outages, such as compliance issues, liability issues, legal issues, public safety issues, data privacy issues, data loss or data corruption, etc.

F. Communication and Coordination

The purpose of this section was to determine each client organization's level of satisfaction with the communications they received during and following the incidents, and their perception of how well the response to the incidents was coordinated.

G Business Continuity Planning

The purpose of this section was to determine whether the various client organizations had any Business Continuity Plans in place for disruption of services or systems, and, if so, whether any of these plans were enacted as a result of the outages.

The survey responses were consolidated into a spreadsheet to facilitate analysis. In addition, EY conducted follow-up interviews with seven key client organizations.

5.2 Survey Questionnaire

Survey questionnaires were sent to the identified client organizations in both English and French. The survey forms were accompanied with clear instructions and the corresponding documents are attached below:

Document Title	Document
Survey email sent to clients – English	Survey
BIA Survey Form – English	Survey
Survey email sent to clients – French	Questionnaire
BIA Survey Form – French	Questionnaire

5.3 Survey Response Summary

The table below represents a summary of survey respondents and related surveys received.

Survey Response Summary	
Number of survey recipients	26
Number of survey responses received	**37**
Departments that did not respond	• Department of Energy and Mines (DEM/MEM) • Department of Natural Resources (DNR/MRN) • Early Education and Childhood Development (EECD/EDPE) • Part II Education (Francophone) – Partial response
Departments that provided multiple responses	• Department of Finance (2) • Executive Council Office / Office of the Chief Information Officer (2) • Department of Agriculture, Aquaculture & Fisheries (2) • Service New Brunswick (8) • Department of Environment and Local Government (2) • Department of Government Services (4)

5.4 Client Organizations Surveyed

EY received 37 completed surveys from the following NBISA clients:

Client Organization	Point of Contact
1. Office of the Premier	, Correspondence & Records Manager
2. Department of Finance - Revenue & Taxation	, Director, Account Management
3. Tourism, Heritage & Culture	, IT Technical Strategist/Analyst
4. Department of Healthy and Inclusive Communities	, Office Manager
5. Department of Health	, Client Relationship Manager/ Operations Manager
6. Aboriginal Affairs Secretariat of the Executive Council Office	, Legislative/Program Officer
7. Executive Council Office (ECO)	, Administrative Support
8. Economic Development (ED-DE)	, Director, Information Management and Technology
9. Invest NB	, Executive Assistant
10. New Brunswick Liquor Corporation/ ANBL	, Director, Information Technology
11. IT Shared Services – Anglophone School Districts	, Director of IT Anglophone School Districts Part 2
12. Department of Agriculture, Aquaculture & Fisheries	, C&E Manager, EMO Coordinator
13. Department of Human Resources	, Manager – Applications and Operations
14. Post-Secondary Education, Training and Labour	, Director, Information Management and Technology Services
15. Department of Finance - Excluding Revenue & Taxation Division	, Director, Information Management and Technology
16. Executive Council Office / Office of the Chief Information Officer	, Director of Operations
17. Efficiency NB	, Energy Efficiency Analyst
18. Department of Environment and Local Government	, Director, Information and Technology Management
19. Department of Public Safety	, Policy Analyst / Strategic Policy and Planning / Department of Public Safety
20. SNB - Corporate Services	, Director of Corporate IT
21. NBISA – Operations & ITaaS	, Director, IT Application Services

Client Organization	Point of Contact
22. SNB - Customer Care	, Executive Director – Customer Care
23. SNB - Corporate Registry	Manager, Corporate Registry
24. SNB - Online Services	, Director, e-Services
25. DGS - Marketing & Web Services	, Director of Operations- Marketing and Web Services
26. DGS - Procurement	, Manager, Procurement Operations
27. SNB - Property Assessment	Regional Director, Property Assessment Services
28. DGS - Provincial Archives	, Director Provincial Archives
29. DGS - Translation Services	Manager, Information Technology and Support Services
30. SNB - Vital Statistics	, Registrar General
31. SNB - Land Registry	, Land Registry Systems Manager
32. Department of Social Development	, Director, Information Technology Services
33. Department of Agriculture, Aquaculture & Fisheries	, Regional Director
34. Department of Transportation & Infrastructure	, Director
35. Francophone School District	, Directeur des technologies de l'information Au service des Districts scolaires francophones
36. Department of Justice / Office of Attorney General	, Director, Justice IMT
37. Department of Environment and Local Government	, Director, Information and Technology Management

Note:
The survey response received from NBISA was completed by internal NBISA organizations not directly providing IT services, e.g. AP, Payroll, Collections.

5.5 Client Organizations Interviewed

It was not feasible to have follow-up interviews with all the client organizations due to the schedule of this engagement and the parameters for conducting the BIA, e.g. objective, level of effort, time etc. Follow-up interviews were conducted with client organizations identified and agreed upon by the Clerk's Committee:

Client Organization	Interview Participants
1. Department of Health	Client Relationship Manager/Operations Manager
2. New Brunswick Liquor Corporation/ ANBL	, Director, Information Technology
3. Department of Finance - Excluding Revenue & Taxation Division	, Director, Information Management and Technology
4. Executive Council Office / Office of the Chief Information Officer	, Director of Operations
5. Department of Public Safety	, Policy Analyst / Strategic Policy and Planning / Department of Public Safety , Director, Information Technology
6. SNB - Corporate Services	, Director of Corporate IT
7. Department of Social Development	, Director, Information Technology Services , Manager, Client Business System Support , Manager, Systems Development & Support , Manager, IT Contract Management , Manager, Executive & Operational Support

Note 1:
It was originally intended to interview the Department of Education (Francophone and Anglophone School Districts) and FacilicorpNB. However, we did not interview the Department of Education because they advised us that, due to the time of year, they were not really impacted by the outages and had nothing to add that was not covered in their survey responses. We did not conduct a separate interview with FacilicorpNB as their issues were addressed as part of the Department of Health responses.

Note 2:
Due to the constraints of time and the availability of key personnel, the number of participants involved in each interview was limited. Hence, the information obtained was limited to the direct knowledge of the participants.

5.6 Key Business Impacts

All BIA survey responses were reviewed and have been summarized below for each section of the survey.

5.6.1 Critical Services and Business Functions

The survey participants were asked to list the critical services and business functions performed by their organization and to describe the potential impacts of an inability to perform each service or function. They were further asked to indicate whether they would consider the impacts to be high, moderate or low based on the following criteria:

a) High Severity: Extended interruption of this service/function affects a wide base of clients, and may have major financial, reputational, regulatory, or health and safety implications. The interruption may have long term consequences.

b) Moderate Severity: Extended interruption of this service/function affects a limited base of clients, and may have some financial, reputational, regulatory or health and safety implications. However, the interruption is unlikely to have long term consequences.

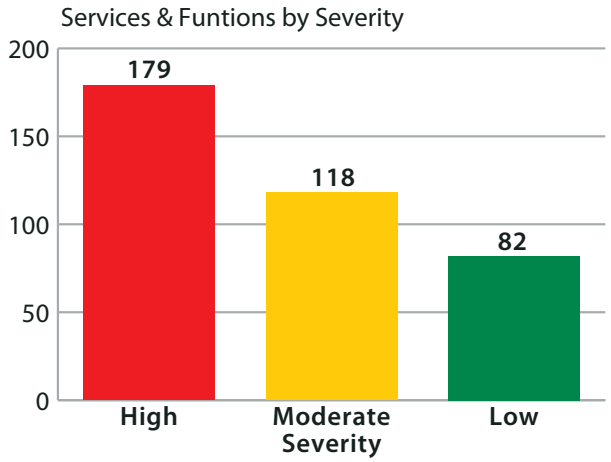
c) Low Severity: The impact is largely internal and has no long term consequences or major financial, reputational, regulatory or health and safety implications.

The following table summarizes the number of services or functions, by department, which could potentially have **high severity** or **moderate severity** impacts if the services/functions could not be performed for an extended period of time.

Department	High Severity	Moderate Severity	Total
1. Department of Agriculture, Aquaculture & Fisheries	2	9	11
2. Department of Environment and Local Government	5		5
3. Department of Finance - Excluding Revenue & Taxation Division	3		3
4. Department of Finance - Revenue & Taxation		5	5
5. Department of Government Services	6	10	16
6. Service New Brunswick	28	26	54
7. Department of Health	26		26
8. Department of Healthy and Inclusive Communities		1	1
9. Department of Human Resource	1	1	2
10. Department of Public Safety	16	36	52
11. Department of Social Development	50		50
12. Economic Development (ED-DE)	2		2
13. Efficiency NB	4	2	6
14. Executive Council Office / Office of the Chief Information Officer	3	12	15
15. New Brunswick Liquor Corporation/ ANBL	3	6	9
16. Office of the Premier	1		1
17. Post-Secondary Education, Training and Labour		5	5

Department	High Severity	Moderate Severity	Total
18. Tourism, Heritage & Culture	7	2	9
19. Department of Transportation & Infrastructure	15	2	17
20. Francophone School District	3	1	4
21. Department of Justice / Office of Attorney General	4		4
Grand Total	**179**	**118**	**297**

The graph below illustrates the number of services and functions categorized by severity:



5.6.2 Essential IT Systems

The survey participants were asked to list the IT systems that are essential to their department's ability to deliver the various services and functions, and indicate whether they would consider use of each system to be of high, moderate or low importance based on the following criteria:

a) High importance: The business service/function cannot be performed without the system.

b) Moderate Importance: The business service/function can be performed without the system, but at a degraded level.

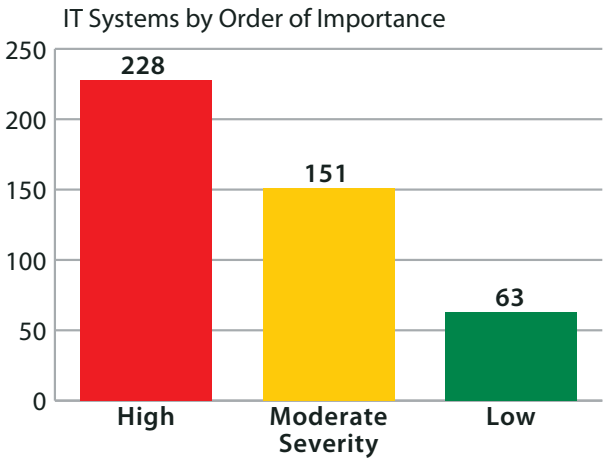
c) Low Importance: Workarounds are available that would enable the business service/function to be performed at an acceptable level without the system.

The following table summarizes the number of IT systems, by department, which were ranked as **high importance** or **moderate importance** with respect to the department's ability to deliver its services or functions.

Department	High Importance	Moderate Importance	Total
1. Department of Agriculture, Aquaculture & Fisheries	5	14	19
2. Department of Environment and Local Government	8		8
3. Department of Finance - Excluding Revenue & Taxation Division	2	3	5
4. Department of Finance - Revenue & Taxation		3	3
5. Department of Government Services	22	10	32

Department	High Importance	Moderate Importance	Total
6. Service New Brunswick	71	51	122
7. Department of Health	16		16
8. Department of Healthy and Inclusive Communities		4	4
9. Department of Human Resource	6		6
10. Department of Public Safety	13	19	32
11. Department of Social Development	29	5	34
12. Economic Development (ED-DE)	2		2
13. Efficiency NB	6	3	9
14. Executive Council Office / Office of the Chief Information Officer	18	14	32
15. IT Shared Services – Anglophone School Districts	3		3
16. New Brunswick Liquor Corporation/ ANBL	10	4	14
17. Office of the Premier	1	2	3
18. Post-Secondary Education, Training and Labour	1	3	4
19. Tourism, Heritage & Culture	5	4	9
20. Department of Transportation & Infrastructure	1	6	7
21. Francophone School District	5	3	8
22. Department of Justice / Office of Attorney General	4	3	7
Grand Total	**228**	**151**	**379**

The graph below illustrates the number of essential IT systems categorized by order of its importance:



5.6.3 Impact of Marysville Data Centre Outages

The following departments indicated that the outages resulted in **High Severity** impacts:

- New Brunswick Liquor Corporation/ANBL
- Department of Agriculture, Aquaculture & Fisheries
- Department of Human Resource
- Department of Health
- Department of Government Services
- Department of Social Development
- Department of Environment and Local Government
- Department of Public Safety
- Economic Development
- Executive Council Office / Office of the Chief Information Officer
- Efficiency NB
- Francophone School District
- Department of Justice / Office of Attorney General

The most pervasive impact reported by the respondents was loss of productivity and reduced service levels. Given the dependence on technology for almost all business functions and services, most staff could not conduct business as usual for varying timeframes depending on which IT systems were unavailable. This was compounded for many client organizations by data loss and corruption on the shared network drives (see section 5.6.5). However, the periods when productivity and service levels were impacted were generally of limited duration (i.e. a few days at most).

In addition to these impacts, some organizations reported external impacts to the public. These were specific to the nature of the services and functions provided. For illustrative purposes, a few of the reported impacts are given below. Note that these responses could not be thoroughly validated as part of this assessment and are reported as received:

Department of Public Safety

The Client Information System (CIS) could not be accessed during the outages. This had a number of impacts, such as:

- Case management information on clients serving sentences in the community (adult and youth) was not available to supervisors of those clients.
- Court ordered probation reports and Victim Impact Statements could not be generated.
- The report listing the clients due to be released from custody could not be generated. Staff had to use manual files to determine who should be released from custody on those days.
- CIS is the primary form used for sentence calculation. During the outages, manual calculations were required for all clients admitted to a Provincial institution.
- Access to Warrants of Committals and Remand Orders was restricted and caused delays in the calculation of sentences and establishing release dates.
- When victims of crime enroll in the Victim Services Notification Process, certain information on incarcerated offenders must, by law, be provided to them. This could not be done during the outages.

The AMANDA system was also down for approximately two days. AMANDA supports a number of core DPS services including licensing and technical inspections. DPS has approximately 45 inspectors and they were not able to input inspection data into the system and hence were not able to issue licenses during the outage, causing inconvenience to the public.

Service New Brunswick (SNB)

The SNB survey response indicated that 39 SNB locations across the province were unable to process customer transactions on June 9th, parts of June 10th through June 14th, and part of June 20th. Most of the service centres had to close during the outages. On-line services were also impacted. This was an inconvenience to the public, particularly for time sensitive transactions such as parking tickets and motor vehicles fines.

Department of Social Development

All Social Development IT systems were unavailable to staff, causing delay in vendor payments and a significant backlog of client data entry needed to be made up at a later time.

As automated safety and security alerts were not available, client files could not be accessed, posing a significant risk to social workers providing Child Protection and Adult Protection Services, as well as to outside service providers delivering social services to Social Development clients.

After hours Emergency Social Services staffs were unable to access their On-Call Workers reports, used for staff scheduling purposes, and were also unable to access safety and security alerts.

Department of Health

For a short period of time, Public Health workers could not determine which vaccines had previously been given to a child.

Department of Justice

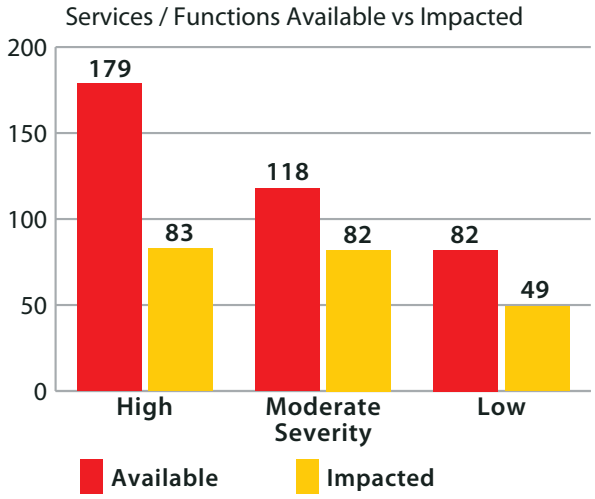
Access to warrant and criminal records was unavailable for a period of time.

New Brunswick Liquor Corporation/ ANBL

Payment card tendering and gift card functionality was impacted on June 9th and 14th. Cash sales remained unaffected.

There is no question that the outages had a broad impact on government services. As illustrated by the graph below, almost half of the highly critical services/functions that are normally available were impacted to some extent, and almost two-thirds of the moderately critical services/functions were impacted.

However, given that the interruptions were limited in duration, the overall impact was serious but not as significant as it could have been if the outages were of longer duration.



5.6.4 Financial Implications of Marysville Data Centre Outages

5.6.4.1 Loss of revenue

From the information provided, loss of revenue was not a significant financial implication of the outages.

Only a few client organizations generate revenue and potentially revenue that was not generated during the outages may have been deferred, not lost, e.g. license fees.

The noteworthy exception is ANBL which generates average daily revenue of over $1M in liquor sales (although actual daily revenue varies depending on the day of the week, time of the year, etc.). ANBL's systems are hosted in the , not Marysville, so they should not have been impacted by the outage. However, when Marysville lost all power on June 9, network redundancy did not function as intended and connectivity to was lost for a few hours. As a result, stores were only able to accommodate cash sales between 10:00 a.m. (store opening) and around noon. The cost, or lost revenue impacts associated with this situation could not be determined through this analysis.

Note:
ANBL experienced a secondary outage of approximately four hours on June 14th. This was not a direct consequence of the Marysville incident, but the result of changes being made by NBISA to Active Directory (the system that enables users to log onto the network) to correct a problem with the system's redundancy Marysville and sites. This outage was more significant since it occurred on a Saturday. Again, stores could only accommodate cash sales while their systems were inaccessible. However, we did not assess the impact of this outage as it was not caused by the Marysville incident and hence was outside the scope of our review.

As indicated previously, loss of staff productivity was cited by most respondents as one of the main impacts of the outages. Several client organizations provided estimates of the cost of the lost productivity as follows:

Department	Cost
Department of Health	$26,840
Executive Council Office / Office of the CIO	$33,268
ANBL	$20,700
Department of Government Services	$29,325
Service New Brunswick	$147,793
Department of Agriculture, Aquaculture and Fisheries	$5,000
Francophone School District	$8,811
Department of Justice / Office of Attorney General	$1,000
TOTAL	**$272,737**

Many other organizations that indicated they also experienced lost productivity could not, or did not provide cost estimates. Assuming that the above estimates represent only a percentage of the actual costs related to lost productivity and in keeping with the intention of determining "order of magnitude" cost impact estimates, the total cost of lost productivity has been broadly estimated to be approximately $500,000.

5.6.4.2 Additional costs

Some departments indicated that they incurred additional costs as a direct result of the outages. The following cost estimates were provided.

Department	Cost
Department of Health	$25,000
Department of Social Development	$49,500
Executive Council Office / Office of the CIO	$850
Service New Brunswick	$72,000
Francophone School District	$3,385
Department of Justice / Office of Attorney General	$300
TOTAL	**$151,035**

5.6.4.3 Incident Remediation Costs

NBISA provided the following estimates of the costs associated with remediating the power-related issues and restoring the Marysville data centre to normal operational status. Note that some costs were asset capital investments that would probably have been incurred at some point in time in the future.

Category	Cost
Employee Costs	$19,115.86
Repairs	$192,685.47
Incidentals	$366,063.84
Capital Investment- UPS (replacement of failed UPS)	$305,173.70
Capital Investment- Automatic Transfer Switch (replacement of failed ATS)	$67,870.70
Other	$16,130.20
TOTAL	**$967,039.77**

5.6.4.4 Total Cost of Incident

From the information collected, the approximate total cost due to the incident is estimated to be in excess of $1.6 million.

Category	Cost
Lost Productivity (approx.)	$500,000.00
Additional Cost	$151,035.00
Remediation including Capital Cost	$967,039.77
TOTAL	**$1,618,074.77**

5.6.5 Other Implications of Marysville Data Centre Outages

As noted above, many departments identified data loss and data corruption as a significant issue resulting from the outages, primarily with respect to their shared drives. The loss or corruption of data required considerable effort to resolve and contributed to the length of time users did not have access to many of their essential files. The Department of Health also reported that there were compliance issues with the Medicare Program related to the use of public folders (i.e. some clients did not receive feedback or follow-up within the guaranteed timeframe).

It should be noted, however, that the data loss/corruption issue was not the result of the outage per se, but the result of systems going down suddenly (i.e. 'hard') due to complete loss of power, without the opportunity to shut down the systems "gracefully".

It should also be noted that more frequent backups of the data could have mitigated the extent of data loss or corruption. For example, Service New Brunswick did not experience data loss or corruption issues since data is regularly replicated (approximately every 15 minutes) the Marysville and .

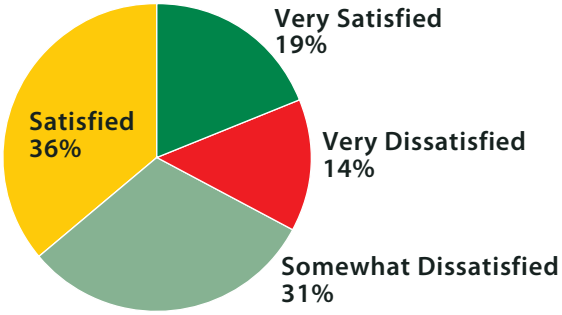
5.6.6 Communication and Coordination

As part of the information gathering conducted through the BIA surveys, feedback on the general level of satisfaction related to incident communication and coordination was sought.

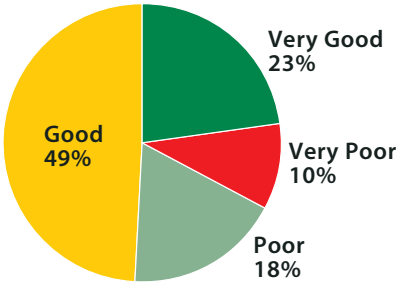
It must be noted that the evaluation does not provide a portrayal of satisfaction by individual client organizations, (from some organizations, several responses were received), but represents feedback from all the received responses. Also important to note is that NBISA feedback, which is included in this representation, is from their non-IT, business services groups, e.g. Payroll, Collections etc.

The level of satisfaction with the communications received during and following the incidents varied by client organization.

As illustrated below, 14% of respondents indicated they were very dissatisfied, 31% were somewhat dissatisfied, 36% were satisfied and 19% were very satisfied.



Similarly, perceptions of how well the response to the incidents was coordinated varied by organization. As illustrated below, 10% of the respondents rated coordination as very poor, 18% rated it as poor, 49% rated it as good and 23% rated it as very good.



Suggestions for improving communication and coordination in a future major incident were provided by some of the respondents. For example:

- *"Regular change management practices were not followed. Technical changes were being made to infrastructure and operations in the background without informing departments. These changes caused numerous technical issues with applications, systems and processes required for day to day business to occur in GNB. Applications issues from users escalated in number, and the troubleshooting of those issues, without realizing what had been done in the background, became very complex, resulting in much longer resolution times for our users. As a suggested improvement, we recommend that standard change management practices remain in effect at all times."*
- *"Coordination, communications and triage were not well coordinated and resulted in many staff being held on 'standby' throughout several evenings and weekends. As a suggested improvement, business continuity and disaster recovery plans for outages should be prepared and tested at least once annually. Client departments should always participate in the testing of these plans."*
- *"An emergency communications plan would improve staff's and the public's perception and expectations during the event."*

5.6.7 Business Continuity Planning

Many of the departments surveyed have some form of Business Continuity Plan in place for events such as loss of facilities, systems, personnel, etc. However, none of these plans were enacted as a result of the outages.

It is worth noting that, at the time of the incident, Service New Brunswick (SNB) had been in the process of implementing a full Business Continuity Plan for loss of their systems hosted in Marysville. Backup hardware had already been installed at NBISA's and data was being replicated regularly from Marysville to . Full implementation of the plan was dependent on 'virtualization' of the servers at Marysville (i.e. replacing the physical servers at Marysville with consolidated hardware that supports multiple servers as virtual machines).

It is also worth noting that, even if this plan had been fully implemented, it likely would not have been activated since the estimated time to restore service at Marysville, after each outage, was less than the time it would have taken to recover all systems at with their planned design architecture.

6 Industry Leading Practices Related To This Incident

6.1 Incident Prevention

Prevention of a major data centre incident, or at least reduction in the likelihood of an incident, is always a critical aspect of data centre design and operation. The higher the availability needs of a data centre, the more stringent the requirements for physical security, power and cooling redundancy, diverse network connectivity, continuous monitoring, etc. However, the higher the needs, the higher the capital and operational costs of building and managing the data centre. Business needs should dictate the level of availability required and should be evaluated based on the criticality of IT systems and the potential impact of downtime.

Data centres are commonly categorized as 'tier 1' through 'tier 4' based primarily on the degree of redundancy built into the data centre. The higher the redundancy, the higher the expected availability (i.e. up time) of the data centre. Following are abbreviated definitions of the four tier levels (per The Uptime Institute).

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure with expected availability of 99.671%
2	• Meets or exceeds all Tier 1 requirements • Redundant site infrastructure capacity components with expected availability of 99.741%
3	• Meets or exceeds all Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure with expected availability of 99.982%
4	• Meets or exceeds all Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%

The difference between 99.671%, 99.741%, 99.982%, and 99.995%, although seemingly nominal, could be significant. For example, a data centre with tier 2 status would allow for 22.7 hours of downtime throughout the course of a year, whereas a tier 3 would only allow for 1.6 hours of downtime.

While the Marysville data centre may have some features of a tier 3 data centre, it could probably best be categorized as tier 2, particularly with respect to its vulnerability to interruptions in utility power. This is not necessarily inappropriate if it has been determined that the cost of maintaining a tier 3 data centre exceeds the potential impacts of downtime and other service recovery measures are in place in the event of site failures.

Another key factor in determining the appropriateness of the tier level is the organization's data centre strategy. If the strategy is to consolidate all critical systems and supporting infrastructure into a single data centre, a higher tier level may be warranted (since all the 'IT eggs' are in one basket). If, however, the strategy is to distribute critical systems or more data centres, a lower tier level may be acceptable (since the impact of a data centre outage would be reduced and the different data centres could serve as reciprocal backup sites for each other).

However, no formal analysis has been done of the tier level requirements for

.

6.2 Incident Response

Regardless of the measures taken to minimize the likelihood of downtime, major incidents affecting the availability of essential systems may still occur. The organization must be prepared to respond efficiently and effectively when they do. Hence, a formal Major Incident procedure should be in place to manage all aspects of a major incident, including resources and communication.

This procedure should describe how the organization handles major incidents, from receiving notification of a potential major incident, through the investigation and problem resolution, to the delivery of a final report summarizing root causes and future preventive measures that may be required.

The typical objectives of a Major Incident procedure are to:

- Provide an effective communication system across the organization during a major incident;
- Ensure that an appropriate Incident Manager and Major Incident Team are in place to manage a major incident;
- Put in place appropriate arrangements to ensure that major incidents are communicated promptly to appropriate management, technical and client groups, so that the appropriate resources are made available;
- Support decision making during the incident response and problem resolution;
- Assign, prioritize and coordinate actions required to contain the incident, correct the root cause, implement contingency measures, etc.
- Monitor and report on the status of all assigned actions, adjusting priorities or resource assignments as appropriate;
- Conduct a review of each major incident once service has been restored and, in line with problem management, to look at root cause and options for a permanent solution to prevent the same major incident happening again.

The Major Incident procedure must also define roles and responsibilities during a major incident. These may vary depending on the organization and the types of incidents covered by the procedure. However, the following are some common roles:

- **Incident Management Team (IMT)**: This is a group of senior IT managers responsible for coordination of the response and key decision making. Depending on the incident, it may also include representatives of the affected lines of business.
- **Incident Manager**: This is the member of the IMT that is in charge of the incident at any given point in the resolution process (i.e. the 'point person'). The role can be handed off from team member to another during an incident of long duration, but there is always only one person in charge. That person should be trained and experienced in incident management.
- **Change Manager**: This is the member of the IMT that is responsible for ensuring that all emergency changes made to the IT environment to resolve the incident are subject to appropriate change controls.
- **Communications Coordinator**: This is the member of the IMT that is directly responsible for coordinating all communications to and from internal and external stakeholders. In large organizations, it may be advisable to establish a separate communications team.

- **Technical Teams**: Specific groups of technical resources deployed by the IMT to investigate and resolve the incident. The appointment of these teams will depend on the nature of the incident and may include external service providers.
- **Service Desk**: Typically, the organization's IT Service Desk will be deployed (under the direction of the Communications Coordinator), to respond to requests for information from affected client groups.

The Incident Management Team should conduct periodic exercises of the Major Incident procedure and any major incidents that actually occur should be subject to a post mortem to identify opportunities for improvement in the handling of major incidents.

At present, NBISA does not have a formal Major Incident Management procedure and does not conduct periodic exercises.

6.3 Incident Recovery

While incident response focuses on resolution of the underlying problem, incident recovery focuses on restoration of the systems and data affected by the outage. Typically, system recovery is time-sensitive, with different systems having different tolerances for downtime. As with data centres, systems are often categorized by tier levels. However, for systems, the lower the tier level, the higher the availability requirements.

Although definitions of tier levels vary from one organization to another, following is a typical structure:

- **Tier 0** – No unplanned downtime. System infrastructure and data are fully redundant in more than one location and all instances are active (i.e. they are all live production systems). If one instance fails (whether due to hardware problems, network failures, or a data centre outage), the other instance(s) continue to operate.
- **Tier 1** – Little or no unplanned downtime. System infrastructure and data are fully redundant in two locations but only one instance is the live production systems. If that instance fails, production 'fails over' to the other instance. This may be fully automated (zero downtime) or require execution of a fail over procedure (downtime of a few hours at most).
- **Tier 2** – Downtime of no more than one business day even in the event of a data centre disaster. Backup infrastructure is in place at an alternate location, and data is backed up to the alternate location at regular intervals (disk to disk). Recovery procedures need to be executed to make the backup system the live production system, but these procedures are usually fairly automated.
- **Tier 3** – Downtime of no more than 2 -3 business days even in the event of a data centre disaster. Like tier 2, backup infrastructure is in place at an alternate location, and data is backed up to the alternate location at regular intervals (disk to disk). However, recovery procedures may require more manual intervention than tier 2 systems. Often the only distinction between tier 2 and tier 3 is that the tier 3 systems are lower priority.
- **Tier 4** – Downtime of no more than one week (even in the event of a data centre disaster). Backup hardware may be in place at an alternate location or may be acquired with short lead time. Data is backed up to the alternate location at regular intervals (typically daily). Recovery procedures may require more manual intervention than tier 3 systems or the systems may simply be lower priority.
- **Tier 5** – Best efforts. Backup hardware is not in place at an alternate location and would have to be acquired. However, data should still be backed up to an alternate location at regular intervals.

NBISA and its stakeholders have not formally assigned tier levels to all systems hosted in the Marysville and . However, the existence of data centres does provide the opportunity to support all of the above tier levels in the event of a major incident at data centre.

Note that, currently, NBISA is only responsible for recovery of the core IT infrastructure. The IT groups within the various departments are responsible for recovery of application systems and data.

7 Key Findings & Recommendations

7.1 Summary of Key Findings

The following represent the key findings resulting from the incident review and Root Cause Analysis (RCA) activities conducted within the scope of this engagement. The findings have been used as the basis for development of relevant recommendations and proposed action plans for the Government of New Brunswick.

Key findings are as follows:

- The data centre incident represented to some degree a "perfect storm" of a series of equipment failures, i.e. Automatic Transfer Switch (ATS), Uninterrupted Power Supply (UPS) unit and standby diesel generator, some of which would not typically be expected – the standby generator, UPS and ATS were maintained and tested, as stipulated by manufacturers.
- Despite the lack of a formalized and defined Major Incident Management process, or a formal Emergency Change Management process, the response measures and decisions taken during the incident to address the multiple equipment failures were appropriate. Given the situation and circumstances, overall the incident was generally well managed:
  - The various participants in the response, including third party vendors and GNB technical and management staff, acted responsibly, collaboratively, and within the scope of their expertise
  - In the absence of defined process, the response team quickly established a command team and decision making and communications structure to be applied during the incident
  - Personnel were particularly resourceful in sourcing and acquiring replacement equipment in an expeditious manner, e.g. second generator
  - Once the severity of the incident was identified, a command centre was quickly established for centralized communication and collaborative decision making
  - Key decisions were based on consensus and seemed appropriate based on the circumstances of the situation and available information that was known at the time.
- Critical data centre facilities infrastructure is aged and approaching end of life (EOL):
  - Facility was supported with a single UPS (no back-up) that was over 22 years old and approaching EOL; notifications of this situation and its risks were made to management in advance of the incident.
  - Other key components of the Marysville data centre facility's support infrastructure, not directly related to the incident, is currently not to leading industry standards:
    - Fire suppression system is only single stage water
    - Cooling (9 Computer Room Air Conditioning units EOL) and
    - Power Distribution Units (PDU's).

  Relevant to the above, it is important to note that other design architecture strategies have been developed to mitigate the above risks, i.e. "dual data centre architecture", but the design has not been fully implemented at this time.
- There exists no formal Major Incident Management process in NBISA for the management and governance of recovery activities during significant IT outages.
- There exists no IT Emergency Change Management process exists in NBISA for management/ governance related to IT configuration changes.
- There exists no defined process or mechanism for NBISA, in the event of a significant IT services issue, to integrate to a broader GNB crisis management process.

- There exist no formal IT Service Continuity Management (ITSCM) plans for key or critical IT services; key IT services have no way of "failing over" to redundant systems in another location:
  - Some systems are designed for high availability and failover, but did not transition as planned/ expected, e.g, Email
  - Suspected DNS/network routing design or configuration issues Marysville and .
- There exists no formal data centre Strategy or Architecture plan for:
  - Site Disaster Recovery, i.e. disaster recovery site from which to recover services
  - High availability and stateful failover (the ability of applications/systems to transition from one set of supporting infrastructure to another without service interruption) of systems data centres
  - Primary/secondary site services assignment
  - Data centre utilization; NB Departments may not be actioning availability of data centre for disaster recovery and high availability.
- There exists no accurate or complete IT applications and services inventory suitable for use in planning and executing IT services recovery:
  - Applications/services are not assigned any criticality rating
  - Applications/services are not prioritized in any way for restoration
  - No SLA's or Availability Tiers established for key IT applications/services
  - Applications/services are not mapped to corresponding support infrastructure.

7.2 Key Recommendations

From the review of events associated with the Marysville data centre incident, the subsequent root cause analysis (RCA), the business impact assessment feedback and EY's general review of current NBISA and broader GNB technology architectures, operational processes and data centre facilities/ services strategies; several recommendations for GNB's consideration have resulted.

The recommendations are intended to mitigate risks to operational IT services currently provided to GNB client organizations from the Marysville data centre and as well identify key opportunities for GNB to develop more cost effective and reliable approaches to the delivery and support of data centre services across the Province.

For each of the recommendations, the relative risk associated with not implementing them has been assessed. Additionally, the approximate timeframes for completion of the recommended actions have been quantified, as feasible, and order of magnitude costs have been estimated.

It is important to note that these initial estimates require further review by GNB, with due consideration being given to several factors relevant to scheduling and cost estimating, e.g. degree of internal vs. external resources utilized, ability of GNB operations staff to support required activities, alignment to GNB strategy etc.

Also note that the recommendations below are not provided in order of priority.

Recommendation #1

Incident recovery activities associated with the Marysville data centre outages were found to be generally well managed, given the situation, however one of the key findings from the Incident Review is the absence of a properly defined, documented and managed Major IT Incident Management Process within NBISA. A major incident management process is integral to governing prompt and effective incident resolution and related decision making and communications. Stakeholder vendors had major incident management processes; however, they were not integrated into any over-arching process managed by GNB or NBISA. The existence of this process would potentially have made incident management more effective.

GNB should formally develop and implement a proper IT Major Incident Management Process to govern recovery activities, communications and decision making during major IT service interruptions. The process should:

- ***Integrate to Emergency IT Change Management processes***
- ***Integrate to any broader GNB Crisis Management protocols or processes***
- ***Incorporate provisions for emergency procurement to support IT incident recovery activities***
- ***Include any third party support organizations involved in or relevant to IT incident recovery activities***.

Following process development, appropriate training should be provided to all process stakeholders and actors, and plans should be developed for the process to be regularly tested

It is estimated that development and implementation activities associated with establishing required processes within GNB would take up to six months.

This recommendation should be treated with a high degree of priority and it is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as high, given the importance of this process in the event of any significant IT service interruptions.

Costs associated with completion of this recommendation are estimated to be less than $250,000.

Recommendation #2

The Incident Review validated that current procedures being practiced in the upkeep, testing and maintenance of key facilities infrastructure, i.e. UPS, generator, ATS, are meeting manufacturer's recommendations. However, given the current data centre facilities infrastructure architecture and design that has only single instances of each of these key components with no designed redundancy, and that some of these key components are aged, it would be prudent to complete a comprehensive review of the current equipment maintenance procedures.

NBISA should initiate a review of current maintenance and testing procedures for key data centre facilities infrastructure, Marysville and The review should address:

- ***Automatic Transfer Switch (replaced at Marysville during recent incident recovery***)
- ***Uninterruptable Power Supply (replaced at Marysville during recent incident recovery***)
- ***Standby Generator***
- ***Power Distribution Units (PDU's***)
- ***Cooling systems; Computer Room Air Conditioning (CRAC) Units***
- ***Systems Monitoring tools***.

The assessments should include review of:

- ***Maintenance frequency***
- ***Methods of procedure (MOP's) for maintenance and testing***
- ***Technician training***
- ***Restoration procedures for equipment in failure situations***.

It is recommended that third party support vendors, and manufactures as appropriate, be involved in the review process.

It is estimated that activities associated with conducting relevant reviews and establishing required processes and standards, would take up to three months.

This recommendation should be treated with a high degree of priority and it is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as high, given the current lack of redundancy in the facilities infrastructure.

Costs associated with completion of this recommendation are estimated to be less than $100,000.

Recommendation #3

The current network architecture the Marysville and did not properly support failover of some key systems/applications that were designed to transition in the event of a service interruption at one site. The cause of this could not be properly investigated, but is understood to potentially be an Active Directory (AD) or related Domain Naming Service (DNS) configuration issue. Activities to investigate this issue are currently in progress. It is important that this issue be fully resolved and tested regularly as this design architecture will make it possible for NBISA to conduct stateful failover of applications and services in the event of operations issues.

NBISA should initiate a review of the current network failover design the Marysville and , and augment the design or configuration as required to support failover of applications/services that are designed with that functionality. Relevant testing should be regularly conducted.

It is estimated that activities associated with conducting relevant design reviews, evaluations and design augments would take up to three months. If further capital equipment purchases are identified as being required to implement a proper design, then timing would be extended for a period of several further months.

This recommendation should be treated with a high degree of priority and it is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as high, given the current lack of redundancy in the data centre facilities infrastructure and that there are several key IT systems/services (email) that have the ability to do stateful failover, if needed.

Unless design reviews determine that new networking or IT infrastructure is required, costs associated with completion of this recommendation are estimated to be less than $100,000. It is important to note that these activities are currently in progress and being actioned.

Recommendation #4

The current electrical facilities architecture for both the Marysville and provides for only single generator back up capability. Given the current incident and experience with generator breakdown, and understanding that timing to implement any newly developed future data centre facilities architecture will not be immediate, having easy access to secondary portable generator capacity in times of major data centre incidents is not that costly and certainly prudent from a risk reduction perspective.

It is recommended that NBISA make provisions, contracting or purchase, for reliable, temporary provisioning of standby portable generator capability to the Marysville and .
This would include implementation of any required facilities electrical infrastructure that may be needed to support a portable standby generator, generator contracting, related fuel contracting, development of implementation processes and related staff training.

It is estimated that activities associated with establishing the noted services and processes would take up to six months. If further capital equipment purchases are identified as being required to implement, e.g. electrical interconnects at the data centre facilities, then timing would potentially be extended for a period of several further months.

This recommendation should be treated with a high degree of priority and it is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as high, given the current lack of redundancy in the data centre facilities infrastructure.

Costs for establishing this capability, assuming no significant capital upgrades are required at GNB facilities, are estimated to be less than $250,000 (this also assumes 3rd party contracting or leasing of this capability).

Recommendation #5

The Province of New Brunswick hosts all of its key data and IT systems within the Province, with of its key data centres in close proximity to i.e. and Marysville.

Given the potential for unexpected events to impact services at these sites, it is recommended that GNB make appropriate plans for recovering key data and IT systems from a distant location, i.e. separate disaster recovery site. Most organizations, given the importance of IT systems to business operations, have established capabilities to recover key IT systems and data from a remote and distant location, independent of normal operating locations. With the Maritime Provinces being a known area for susceptibility to severe environmental events such as hurricanes, it is recommended as prudent for GNB to consider establishing these capabilities for identified critical IT systems/services.

Within the context of a broader data centre architecture plan for GNB, it is recommended to develop appropriate disaster recovery site capabilities for key identified IT systems/applications. Once established, it is important to plan for outage situations and regularly conduct disaster recovery exercises.

It is estimated that activities associated with establishing the required services (often through a 3rd party provider) and processes would take up to twelve months.

This recommendation should be treated with a high degree of priority and it is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as high, given the current lack of redundancy in the data centre facilities infrastructure and potential for data centre outages in the future.

Costs for establishing this capability, assuming IT infrastructure capital equipment purchases will be required, are estimated to be less than $1,000,000.

Recommendation #6

In the process of conducting the RCA for the data centre incidents, key facilities infrastructure at the Marysville data centre was identified as approaching or potentially being past "end of life" (EOL), aged and posing risk to IT services. During the recent Marysville data centre incident, several key facilities infrastructure components were replaced as part of incident recovery activities, i.e. UPS, ATS, but there are still several components that should be further reviewed and assessed for potential replacement; examples include PDU's and CRAC units that are past end of life.

Review and any resulting recommended capital investment should be conducted in alignment with the broader data centre architecture strategy referenced in Recommendation #8.

It Is recommended NBISA conduct a review of other key potentially aging and suspect data centre facilities infrastructure, conducting a risk analysis to determine if replacement, upgrade or other capital investments should be actioned, e.g. aged and EOL PDU's, fire suppression system, CRAC units.

Additionally, it has been noted that NBISA does not have an ongoing, funded program for IT infrastructure "refresh", i.e. a "Keep Environment Current" program. It is recommended that GNB consider establishing an appropriate sinking fund to address aging IT infrastructure replacement needs.

It is estimated that activities associated with conducting this review would take up to three months.

This recommendation should be treated with a moderate degree of priority and is recommended to be actioned as soon as practicable by NBISA. Risks associated with not implementing are ranked as moderate. One interim approach to mitigate risk would be to identify any critical IT systems currently being supported by identified equipment for review and assessing options for transition.

Costs for conducting this review are estimated to be less than $100,000. Costs for potential capital equipment upgrades cannot be determined at this time, but potentially could be greater than $1,000,000.

Recommendation #7

Currently, there exists no up-to-date database or inventory of applications being hosted at GNB data centres, with the applications being properly mapped to supporting infrastructure.

This situation impacts the organization's ability to effectively design and provision appropriate infrastructure for supporting applications appropriately, based on their availability needs.

This situation also impacts the organization's ability to effectively restore key applications/systems in the event of any data centre incidents. Additionally:

- Applications/services are not assigned any criticality rating
- Applications/services are not prioritized in any way for restoration
- No SLA's or Availability Tiers are established for key IT applications/services
- Applications/services are not mapped to corresponding support infrastructure.

All of the above information is typically required to properly and cost-effectively design supporting infrastructure for applications and implement required service continuity plans. Additionally, this information is integral to successfully developing a GNB data centre facilities strategy (Recommendation #8).

It is recommended GNB develop a complete listing of applications and services supported by GNB data centres, developing processes for maintaining their accuracy/integrity. Formal Availability Tiers for should be assigned for all key systems and applications (Business Impact Analysis data can be used as a starting baseline) in preparation for the development of supporting IT service continuity management and disaster recovery plans.

Also, going forward, any new application development/implementations should have their availability needs defined and the requirements incorporated into their respective designs.

It is estimated that activities associated with completing this activity would take up to six months.

This recommendation should be treated with a high degree of priority and is recommended to be actioned as soon as practicable by NBISA. Risks associated with not implementing are ranked as moderate.

Costs for conducting this review are estimated to be less than $250,000.

Recommendation #8

With new technologies available to enterprise IT organizations enabling significant server and storage infrastructure consolidation, data centre infrastructure and facilities optimization is a high priority for IT departments and is accepted as the most important opportunity for long-term cost reduction and IT service performance improvement.

Server and storage technology consolidation is a key consideration in determining requirements for data centre facilities space/power needs.

Governance and operational management of data centre services is also an important aspect of any forward looking strategy for data centre facilities and should also be reviewed.

Disaster recovery and ITSCM planning are also key drivers of facilities requirements and need to be incorporated into strategy development.

Prior to initiating any further significant capital investments into current NBISA data centre facilities to increase resiliency and mitigate service outage risks, and prior to concluding any long-term managed services agreements incorporating commitments from GNB, it is recommended that a comprehensive review of the current GNB data centre facilities architecture, applications/server technology current state, operational management model and governance practices for GNB data centre services be completed, developing a strategy that will reduce risk to IT services, improve services to GNB client organizations and reduce data centre services costs.

It is recommended that GNB develop and implement a comprehensive data centre facilities strategy for all of its hosted IT systems. The strategy should develop facilities requirements based on:

- ***All GNB application hosting needs (not just NBISA***)
- ***Technology optimization/consolidation opportunities***
  - ***Storage***
  - ***Server***
- ***High availability failover needs***
- ***Synchronous data transfer needs***
- ***Disaster Recovery needs***
- ***Application availability needs/tiering***

Various governance, facilities, operational management and managed services options should be considered in development of the overall facilities strategy – the strategy should have the key objectives of improving IT services performance and reliability and reducing long-term costs for data centre services.

It is estimated that activities associated with completing this activity would take up to six months.

This recommendation should be treated with a high degree of priority and is recommended to be actioned as soon as practicable by GNB. Risks associated with not implementing are ranked as moderate.

Costs for development of this strategy and program are estimated to be less than $250,000.

Recommendations Overview

The following table summarizes key recommendations providing initial estimates of activity duration and cost (these estimates must be recognized as preliminary and requiring further evaluation and refinement by GNB).

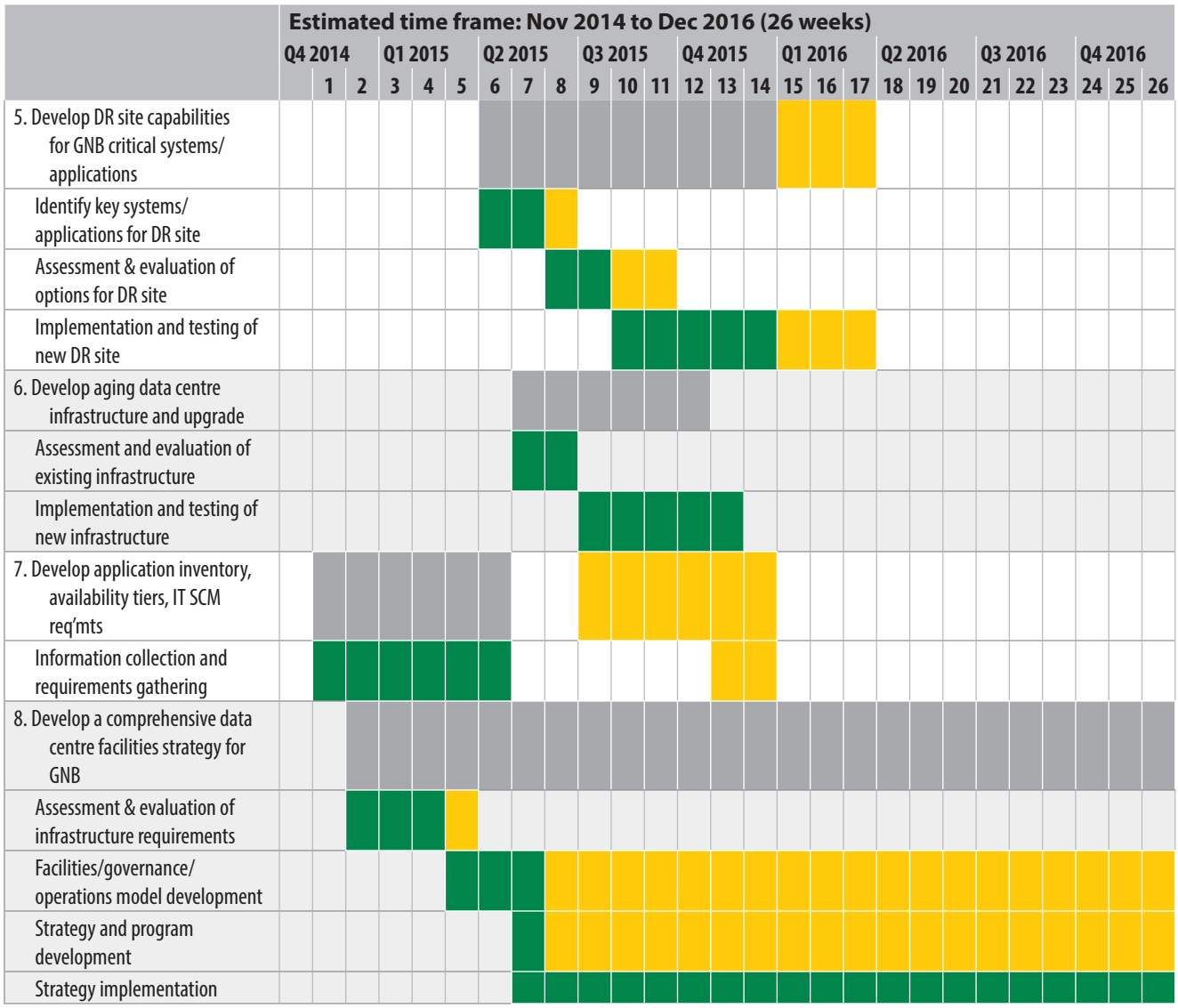
Recommendation	Duration (Months)		Cost ($ < 100K, $$ < 1M & $$$ > 1M)		Priority	Risk Rating
	Planning (up to)	Implementation (up to)	Planning (up to)	Implementation (up to)		
1. Develop Major Incident Management Process	4	2	$	$	High	●
2. Review Current Maintenance/Testing Procedures	2	2	$	$	High	●
3. Establish Network Failover Capability	2	6	$	$$	High	●
4. Establish Portable Standby Generator Capability	2	4	$	$	High	●
5. Establish Disaster Recovery site	3	9	$	$$	High	●
6. Review Other Aged, EOL Marysville DC Infrastructure	2	10	$	$$ -$$$	Medium	●
7. Complete Application Inventory and Availability/ Criticality Assignment	4	2	$$	$	High	●
8. Develop data centre Facilities Strategy	6	TBD	$$	TBD	High	●
					Risk Rating	● High ● Medium ● Low

7.3 Prioritized Action Plan

For the defined recommendations, EY was asked to provide a preliminary prioritized roadmap for recommended remediation activities to be considered by GNB. The following preliminary schedule has been developed to aid in understanding the recommended priority associated with each of the recommended actions and the potential scheduling that could be adopted for actioning the recommendations, taking into account related dependencies.

It is important to note that this schedule requires further assessment and evaluation by GNB, incorporating consideration for numerous other factors that are relevant to appropriate schedule development.

	Estimated time frame: Nov 2014 to Dec 2016 (26 weeks)																									
	Q4 2014		**Q1 2015**			**Q2 2015**			**Q3 2015**			**Q4 2015**			**Q1 2016**			**Q2 2016**			**Q3 2016**			**Q4 2016**		
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
1. Develop Major Incident Management Process																										
Assessment & evaluation of existing processes																										
Process Integration and Implementation																										
2. Review maintenance procedures for key data centre infrastructure																										
Assessment & evaluation of current procedures																										
Development Planning for maintenance and testing																										
Training, communication and implementatio of new procedures/practices																										
3. Review & re-configure failover design data centres																										
Assessment & evaluation of existing failover design																										
Planning/implementation of failover architecture																										
4. Develop portable generator capabilities at NBISA data centres																										
Contracting and design planning																										
Planning and implementation of portable generator capabilities																										


Estimated time frame: Nov 2014 to Dec 2016 (26 weeks)
Q4 2014
Q1 2015
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Q2 2016
Q3 2016
Q4 2016
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
5. Develop DR site capabilities for GNB critical systems/ applications
Identify key systems/ applications for DR site
Assessment & evaluation of options for DR site
Implementation and testing of new DR site
6. Develop aging data centre infrastructure and upgrade
Assessment and evaluation of existing infrastructure
Implementation and testing of new infrastructure
7. Develop application inventory, availability tiers, IT SCM req'mts
Information collection and requirements gathering
8. Develop a comprehensive data centre facilities strategy for GNB
Assessment & evaluation of infrastructure requirements
Facilities/governance/ operations model development
Strategy and program development
Strategy implementation