

CURRENT STATE ASSESSMENT

OPERATIONS SCORECARD

OVERALL RATING

Overall Health Check Rating is based on the rolled-up score of all areas defined within Operations: IT Governance, IT Service Management, and Business Continuity Management.

IT Infrastructure Health Check: Operations





May 16th, 2017

Last Year	IT Governance – IT Service Management – Business Continuity Management	Health Check Rating
N/A		2.3

IT GOVERNANCE

VALUE SCORECARD

OPERATIONS

RATING LEVELS	IT GOVERNANCE	 LEVEL OF ACCEPTANCE	 BUSINESS ALIGNMENT	 OBSOLESCENCE	 COST \ EFFORT
3 HIGH	Governance Framework				
2 MEDIUM	Operational Security Policy				
1 LOW	Risk Management Policy				
	Backup & Recovery Policy				
	Cloud Computing Policy				
	Standard Operating Procedures				
	Project Portfolio Management				
	Vendor Management				

ITEM

CURRENT RATING

PREVIOUS RATING

¹IT GOVERNANCE

2.0

N/A

Synopsis:

Although the Region appears to have several sub-committees designed to support project activities, there is no formal IT framework for the governance and management of enterprise IT.

Key IT policies have not been developed with the exception of Risk Management which is present at the corporate level and has included an overall IT Risk Assessment. However, Security, Backup\Recovery, and Cloud, are examples of core areas where the Region requires policy development.

IT Standard Operating Procedures (SOPs) appear to be non-existent resulting in the dependence of the tribal knowledge of a small group IT resources.





Projects follow a consistent methodology that includes reporting and communication with stakeholders and the Corporate Technology Steering Committee.

Please refer to the [IT Governance](#) section for the complete review and recommendations

¹ IT Governance - our assessments include a complete review of IT Governance, benchmarked against industry leading frameworks such as Control Objectives for IT (CobIT). IT Governance ties IT goals to those of the enterprise. It ensures that IT delivers valuable services through the optimal use of its resources, while understanding the risks involved and the establishment of goals and metrics to track organizational performance.

IT SERVICE MANAGEMENT (ITSM)**VALUE SCORECARD**

OPERATIONS

RATING LEVELS	IT SERVICE MANAGEMENT				
		LEVEL OF ACCEPTANCE	BUSINESS ALIGNMENT	OBSOLESCENCE	COST \ EFFORT
3 HIGH	Incident Management Lifecycle				
2 MEDIUM	Service Desk (Helpdesk)				
1 LOW	Change Management				
	Knowledge Management				
	Problem Management				
	IT Asset Management				
	Configuration Management(CMDB)				

ITEM CURRENT RATING PREVIOUS RATING

ITSM

2.7

N/A

Synopsis:

The Service Desk has some structure, with users able to submit requests in a formal ticketing system with issue tracking. However, there needs to be some development around a tiered support model (i.e. Service Desk vs. Helpdesk).

In addition, fundamental best practices around the management of incidents and problems needs to be improved. For example, the terms “incident” and “problem” appear to be used interchangeably, although they are considered two distinct processes within the IT Service Management (ITSM) framework.

Knowledge management is currently based on an ad-hoc system (OneNote) which is not considered best practice. However, the Region is currently in the process of migrating to a formal system.





IT Asset Management is ad-hoc and requires additional work in order to properly track hardware and software assets within ITS. A Configuration Management Database (CMDB) to support, among other things, both change and incident management, would be beneficial in the support of IT assets within the Region.

Please refer to the [ITSM](#) section for the complete review and recommendations

BUSINESS CONTINUITY MANAGEMENT (BCM)

VALUE SCORECARD

OPERATIONS

RATING LEVELS	BUSINESS CONTINUITY MANAGEMENT				
		LEVEL OF ACCEPTANCE	BUSINESS ALIGNMENT	OBSOLESCENCE	COST \ EFFORT
3 HIGH	IT SERVICE CONTINUITY MANAGEMENT				
2 MEDIUM	Backup and Recovery				
1 LOW	Disaster Recovery				
	IT Enterprise Risk Management				

ITEM	CURRENT RATING	PREVIOUS RATING
BCM (ITSM)	2.1	N/A

Synopsis

IT Service Continuity Management (ITSCM) is designed to support the overarching Business Continuity Program.

The Region made some investments in the development of a Business Continuity strategy, however much of the work in this area – specifically related to Disaster Recovery – has become outdated.

Business Impact Analysis’ were conducted back in 2015 and will require a refresh. There is no formal IT Risk Management strategy in place to support an overarching BCM program.

Although there are DR procedures in place for some systems, these procedures have not been tested.

System backup and recovery procedures are in place but need to be formally documented. The current lack of data management lifecycle processes has also added to the high cost of managing the backups.

Please Note: There does appear to be a group responsible for the corporate Business Continuity program, however there is limited communication between this group and ITS.

Please refer to the [Business Continuity Management](#) section for the complete review and recommendations

FINDINGS AND RECOMMENDATIONS

ORGANIZATIONAL REVIEW

CURRENT STRUCTURE (INFRASTRUCTURE AND OPERATIONS)

Demand for technology solutions continues to grow exponentially, however most municipal IT teams are perceived as being a “solid utility” by staff and management – responsible for supporting core technologies and “keeping the lights on”. The Region is faced with a similar challenge, with key resources bogged down with day to day issues that prevent them from spending an appropriate amount of time on strategic initiatives and the development of best practices. Looking to the future there is a significant opportunity at the Region for developing the role of IT, allowing them to become a true “partner player”.

The reality of modern IT is that maintaining the necessary skills and capacity to manage an increasingly complex technical environment and burgeoning project demands in-house is impractical. To do so would mean hiring an unfeasible number of additional IT staff.

Smart IT organizations rely on a team of in-house IT staff, who in turn work with a network of trusted partners, vendors and solution providers to deliver the required services. The focus is on “getting it done” rather than IT staff always doing it themselves.

This is a *hybrid model* of IT service delivery, that combines internal IT and business skills with market based expertise and services. Ultimately it means that the IT team, the Director and IT Managers act more as coordinators or strategic orchestrators of IT service delivery – which is delivered by internal and external providers.

Service Providers: Out-Task Some IT Services

Some of the Regions IT systems are tailored to a specific municipal line of business. However, many technologies that the Region runs (such as networks, servers, file storage and email) are more generic. As hospitals, construction firms, banks and other organizations have come to use the same systems these areas of IT have become more commoditized making direct services available on the open market. Private sector firms can be used to manage, operate and support some, part or all of these services on behalf of municipalities.

As an example, specialized security expertise which is often required but not necessarily on a fulltime basis is accessed on an “as needed” basis from outside firms. These services will be used to augment existing IT resources, and will be used to manage and implement technologies that current IT staff don’t have detailed domain expertise in or capacity to deliver.

Another example would be a migration to Microsoft Office 365 for email services. When you consider the costs associated with supporting the current Exchange infrastructure at the Region (*hardware, software, staffing*), moving these services to the Microsoft cloud would not only result in a decrease in operational costs, but resources supporting this infrastructure would now have the cycles to focus on other IT initiatives.

IT as a Partner Player: The Need for Strategic Development

The current organizational structure within IT does not account for strategic development, resulting in the Region’s low ratings in areas such as policy and procedural documentation, disaster recovery, and infrastructure roadmaps. Please see Figure 1 below:

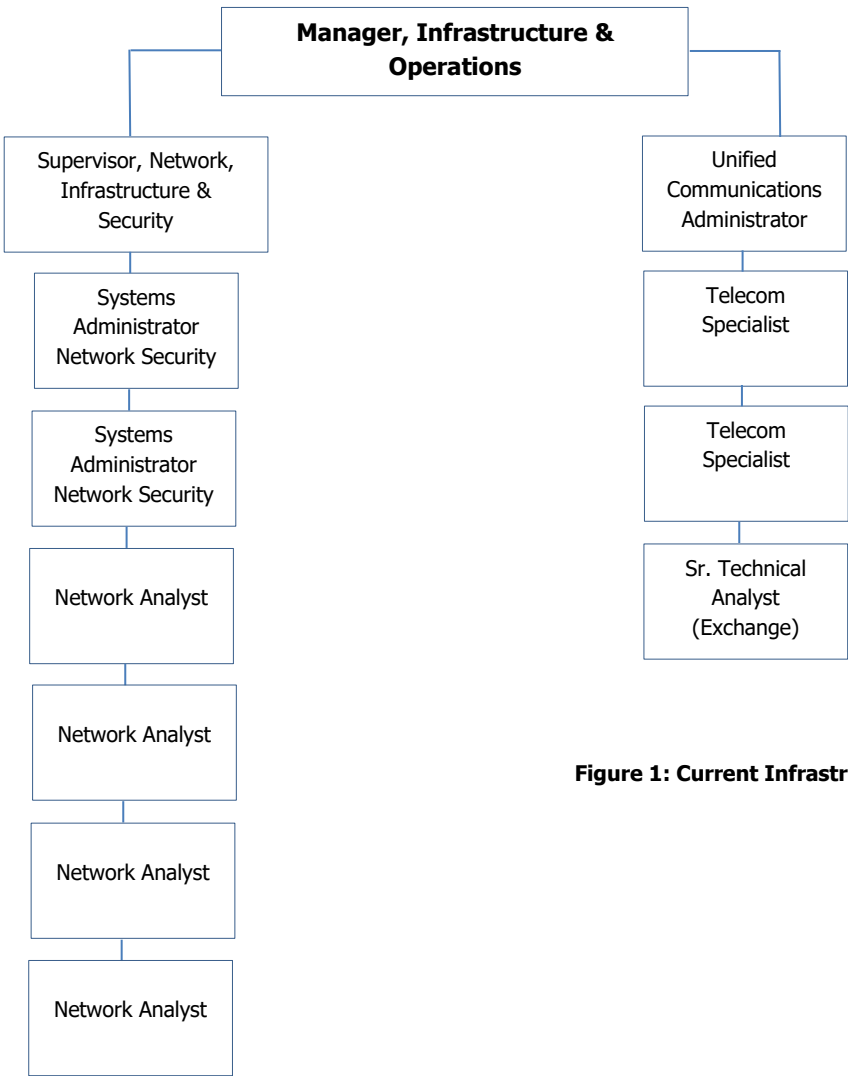


Figure 1: Current Infrastructure and Operations Organizational Chart

Based on our assessment of resources currently working within Infrastructure and Operations, and the challenges faced, we're recommending the Region move forward with an organizational strategy as follows:

1. Create a new team focussed on "Infrastructure Strategy and Development".
 - a. Three current staff would be moved into this group (*see Figure 2*)
2. Move forward with the key recommendations in this report that address the primary requirements within the Region (see [Budget and Roadmap](#))
 - a. Utilize "out-tasking" as needed (refer to previous page) in order to ensure tasks are completed in a reasonable amount of time
3. Once the key recommendations are completed review the landscape within Infrastructure and Operations and determine if an FTE (fulltime equivalent) is required to address a need for specific skillsets best served by an "in-house" resource.
 - a. Do not hire any FTE's until the requirements have been determined after the "cleanup"
 - b. Consider hiring a consultant on a 1-year contract with skills in: VMware, networking (intermediate), enterprise storage management

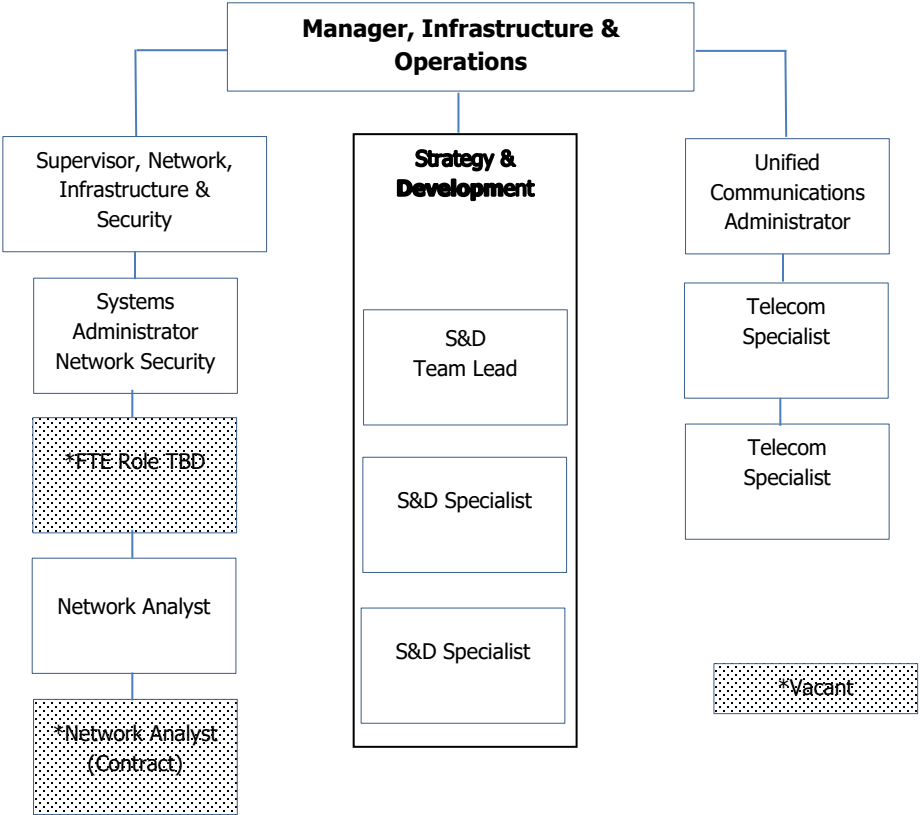


Figure 2: Proposed Infrastructure and Operations Organizational Chart

OPERATIONS

IT GOVERNANCE

IT Governance is the processes and structures which inform, direct, manage, and monitor how the organization makes the best and most effective use of technology.

An IT governance framework is designed to ensure that the right people are making the right decisions, at the right time and for the right reasons. It is also important that everyone in the organization understands how technology decisions are made, priorities set so that they can add their ideas into the mix in the right way.

In some cases, IT decision making means collective decision on corporate priorities, in other areas it will involve technical decision making on the best data storage technology or networking protocol – thus different groups, with different skill sets need to be involved.

Organizations often view decisions about technology as complicated, technical and “best left to the experts in IT”. However, in a surprising number of cases, decisions about technology have ramifications, well beyond the technology itself:

- How do we want to use technology in our business?
- What technology do we want our people to use, and how do we want them to use it?
- How much should we spend on technology?
- Which of our business processes should we direct our IT dollars towards?
- What do we need to tackle first?
- Should we do this now, or later?
- How secure do we want to be?
- What should be available first in the event of a data centre outage or a disaster event?

These are not decisions that technologists alone should be making, they are important business decisions that the leaders of the organization must address. There are of course purely technical decisions to be made, and the right IT staff (with the appropriate skillsets) need to be involved – but in most cases IT experts should be advising business leaders.

Perhaps more important is the cultural and business change and learning that is necessary to take full advantage of technology. It is important that business leaders learn what’s possible, and learn from other projects what it takes to be successful. Governance models allow this type of learning to be internalized.

What is an IT Governance Model?

IT governance models should facilitate collaborative working, bringing together staff from various departments and disciplines. IT governance is a combination of:

- Decision making groups and individuals (e.g. membership, inter-relationships)
- Policies & standards (e.g. architecture, software procurement policy)
- Processes & methods (e.g. prioritization, project execution)
- Measurement and monitoring (e.g. KPI reporting)

Although the Region appears to have several sub-committees designed to support project activities, there is no formal IT framework for the governance and management of enterprise IT. There are job descriptions that define roles and responsibilities and signing delegation of authorities. The Director of IT has lowered the authorities for 2017 to afford a means of better understanding and questioning many of the status quo that routinely occurs.

There are various committees that are documented for project activities, however there is not a general framework.

While the model is a good foundation, several opportunities to improve the Regions governance of technology could be implemented, including:

- Roles and responsibilities of each group could be more clearly defined
- Corporate IT policies must be updated
- Additional groups, including an Architecture Review Board and standing Steering Committees Groups should be added to the existing groups
- The formal annual intake process should be reviewed to allow more agile responses to mid-year projects
- More comprehensive portfolio information on operational / technical infrastructure projects should be shared with an IT Steering Committee (ITSC).

Add an Architecture Review Board

The Architecture Review Board is responsible for coordinating the development of architectural standards. The Board also reviews all technology and business initiatives to monitor compliance with the standardized architecture, and makes recommendations to project teams, sponsors, the IT Management Team, and ITSC.

IT POLICIES

Policies and standards should establish the parameters within which the Region uses technology, creating clear expectations for those that use and manage technology. In keeping with the commentary throughout this section, many of the decisions related to technology are business or management decisions. These are not decisions to be made by IT on behalf of the corporation. For example;

- Which employees get smartphones
- Who is authorized to register a web domain for the Region
- Which websites staff can access, and whether that activity should be tracked
- What content is saved when an employee retires
- How much space does an employee have in email

For each of these decisions several factors need to be weighed, including business impacts, employee impacts and importantly, cost impacts. A standard IT policy framework typically addresses the following areas.

- Acceptable use
- IT Security
- Backup, recovery, BC and DR
- Asset lifecycle management
- Hosted and cloud solutions
- Data management (lifecycle, privacy)
- IT procurement processes
- Email & voicemail standards (including archiving)

While the Region has a few of these policies, most require updates. IT Management, with the input of staff, stakeholders and ITSC should review, revise and augment the corporate IT policy framework in the context of this strategy, to ensure that it accurately reflects how the Region wishes to use and manage technology. A leadership team needs to be responsible for reviewing and approving policies recommended by IT Management/ITSC.

IT ARCHITECTURE

IT Architecture is one of the most important standards. At a high level the Architecture represents core concepts that underpin this strategy that the Region will pursue. The IT Architecture represents a macro level blueprint, the Official Plan if you will, for how the IT environment is to be developed and built.

More detailed current and to-be architectures (the equivalent of secondary and community master plans, to carry on the analogy) have been, or will be, developed by the Regions IT team for the Infrastructure, Application, Integration, Data and Business Process layers of the architecture.

These plans, through the work of the **Architecture Review Board** will ensure that new solutions can be designed and implemented in a way that appropriately integrates with existing solutions.

Solutions, Network and Technology Architect roles will be established within the IT department and will have the delegated authority from the IT Management team to review solutions for architectural fit.

IT STANDARDS, GUIDELINES AND PLAYBOOKS

In addition to the IT Architecture the IT Management team will lead the development of guidelines and playbooks to simplify and delegate IT decision making to project teams and staff. Examples include:

- IT service catalog
- Device guidelines, and associated requests / approval processes
- Cloud playbook
- Security assessment process
- Project initiation playbook
- Change management playbook
- Business process design playbook

Internal to IT, documentation of IT technical standards and SOP's (Standard Operating Procedures), are important internal documents and tools to help the IT team deliver its mandate and comply with policy directives. IT documentation, though currently adequate where it exists, should be improved by the IT Team. The team should determine where the knowledgebase will be managed. At a minimum, SOP's for the following areas should be in place:

- Incident management
- Change control process management
- Backup and recovery,
- Problem management
- Security management,
- Configuration management of critical systems

IT SERVICE MANAGEMENT (ITSM)

IT Service Management has some structure in the following areas:

1. Service Desk (Helpdesk) – Fairly well managed with a central point of contact supporting all regional sites
2. Registration of Customer Queries – Clients are able to submit a request via a self-service webform or by phone.
 - a. All requests are logged in ticketing system and classified
 - b. SLAs are attached to each type of request - requests and incidents. Customers are able to track the status of their request via the self service portal.
3. Knowledgebase
 - a. Currently using an ad-hoc system (OneNote) which poses some security concerns.
 - b. Once existing documents are migrated to ticketing system the Region will look at adopting a structured approach to maintaining information and will target updating and reviewing articles on a regular basis (based on use and importance of the article).
4. Service Catalog – In the process of being updated

Some key areas that require attention include:

1. Proper definitions of ²“incidents” vs “problems”
2. Incident Escalation – This appears to be on a best effort basis
 - a. The Region does not have defined thresholds or criteria for request/incident escalation - other than the SLA triggers in the system that notify when an incident has breached it's SLA.
 - b. There is an approved draft for incident escalation and notifications but work is required with the system vendor to integrate into system.
 - c. This process however does not define the criteria for escalation, i.e. what steps needs to be taken at tier 1 and 2 and what thresholds need to be met prior to escalating a ticket to another IT group - Tier 3.
3. Asset Management – This appears to be an ad hoc process although the Region recently migrated hardware inventory into a new system and have a defined ongoing maintenance process.
 - a. They are currently in the process of validating the accuracy and are making updates to correct issues.
 - b. Software licenses can be reported on and can be tied to a machine but are not formally tracked or in the same systems as the hardware inventory.

² According to ITIL, an **incident** is an unplanned interruption to a service or a degradation in the quality of a service. What often determines the classification of something as an incident is whether or not the service level agreement (SLA) was breached. However, ITIL allows for raising an incident even before an SLA has been breached in order to limit or prevent impact. A **problem** is defined as the root cause of one or more incidents. Problems can be raised in response to one or more incidents, or they can be raised without the existence of a corresponding incident.

4. Reporting and Trend Analysis - There are defined metrics at a team (KPI) level and high level however neither are regularly tracked or reviewed.
 - a. This needs to become a standard process
5. Change Status Tracking and Reporting – Although the actual CM process appears to be well managed, they appears to be no reporting to senior management.
6. Monitoring and Reporting Against SLAs – As one point the Region reported on standard regional KPI's and had developed more ITS internal KPI's and reported on them but this process stopped 2 years ago.
 - a. The Region needs to reignite this process

Recommendations

- Clarify the role of the **Service Desk** – ensure that it follows ITSM best practices framework

The service desk was an evolution of the helpdesk, born out of the ITSM best practice framework ITIL, and based on the underlying concept of “managing IT as a service.” The terms are often used interchangeably, but it’s important to note that Helpdesk is now considered a *sub-set* of a Service Desk; The process concerned with resolving issues using the break/fix concept.

A Service Desk is more strategic term - it's not just about “fixing stuff”, but also about adding new services and maintaining the existing ones.

- Separate and distinguish support roles within ITS - Incident Management & Problem Management

Incident Manager or Service Desk Manager

Within the IT Service Operation part of the ITIL Service Lifecycle, the Service Desk function is the core, acting as a single point of contact for all end users. The Service Desk usually logs and manages all incidents and service requests, and provides an interface for all other Service Operation processes and activities. The Service Desk is the key to the implementation of the Request Fulfillment and Incident Management processes. It’s important to understand that Incident Management is a cross-IT organization process, not a Service Desk-only process.

As illustrated in **Figure 3**, the recommendation is that the Region refine its support model to ensure adherence to ITIL best practices pertaining to ITSM.

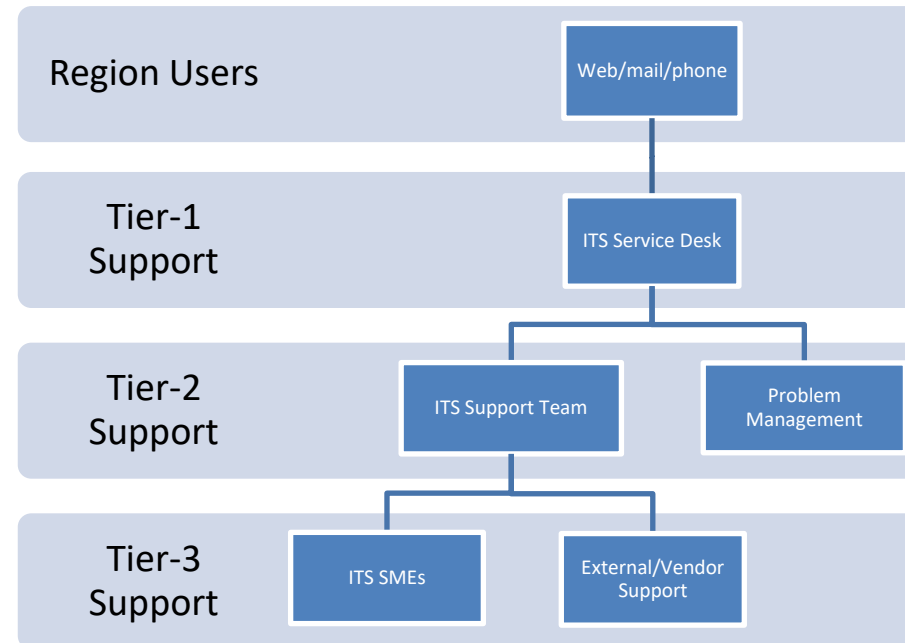


Figure 3: Example of role separation with ITS for the Incident Management process. While Problem Management does not support Region users directly, it is responsible for finding and eliminating the root cause of an incident.

Tier-1 Support / Service Desk

As illustrated, ITS Service Desk is involved in the Incident Management process, in the role of **Tier-1 Support**. Once end users contact the Service Desk, ITS Service Desk attempts to collect as much information and diagnostics about the incident as possible, and even resolves the issue on the spot, if possible. This will reduce resolution time for all minor incidents (q: my computer doesn't work – a: did you try to turn it on?), and first-contact resolutions consequently increase end user satisfaction.

In general, Tier-1 support staff within ITIL Incident Management will be managed by a **Service Desk Supervisor (or equivalent)**, who will also serve as the escalation point, if needed. If Tier-1 Support is not able to resolve the incident right away, it will escalate the incident to **Tier-2 Support**.

Tier-2 Support / Service Desk

Tier-2 Support of Incident Management is a role generally composed of the staff with greater technical skills than those of Tier-1. They should have enough time on their hands to devote themselves to incident diagnosis and resolution. Tier-2 Support will pay a visit to Region staff if required, something that Service Desk staff can't do.

One common example, is fixing or setting up a projector in a conference room(s), or providing enough cables and enabling network access for all computers in a conference room. The Service Desk, in this situation, can't help remotely – you wouldn't send someone from the Service Desk to do it, as at some point you wouldn't have any Service Desk personnel left to answer the phone / e-mail and provide the first level of support.

Tier-3 Support / Service Desk

The **Tier-3 Support role** is typically reserved for external suppliers and vendors; however, within the Region there are several resources that would/could be considered "subject matter experts"; e.g. network support, VMware support, hardware maintenance, etc.

BUSINESS CONTINUITY MANAGEMENT (BCM)

IT SERVICE CONTINUITY MANAGEMENT

As a subset of the Business Continuity Plan, IT Service Continuity Management (ITSCM) proactively assures IT services can be recovered and provisioned based upon the established business continuity management timeframes. Basically once you rate your critical applications, assuring the critical are up first within the agreed upon timeframe. This helps to have a pre-defined process in place to help the organization recover to normal operating procedures after a disaster. On the reactive side of the equation, once the disaster has occurred. IT service continuity management is the process responsible for assessing the impact of the disruption on IT services.

Backup and Recovery

ITSCM considers application backup and recovery one of the risk mitigating factors in assuring service continuity.

Currently the Region does not have a formal Backup & Recovery strategy, although they do have an enterprise class backup system (CommVault). The solution has proven to be quite costly which further drives home the requirement to analyze the current data being backed up in order to classify “active” vs. “inactive” for archiving purposes (lower/cheaper storage).

This process will also help with the issue of slow recovery’s and long backup times.

Business Continuity (Disaster Recovery & IT Enterprise Risk Management)

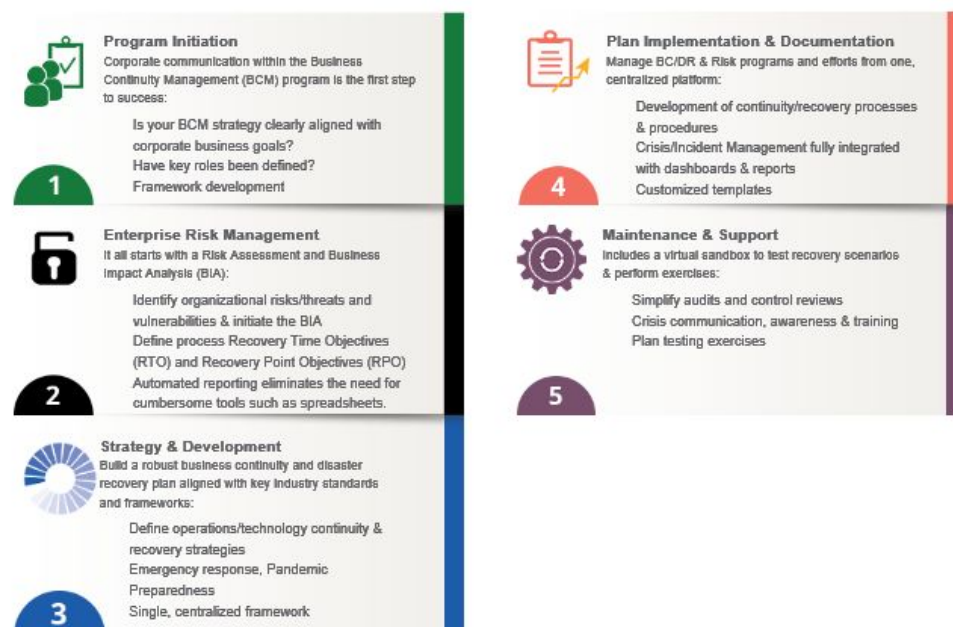
For municipalities such as the Region of Waterloo, service disruptions, delays in responding to customer requests, inability to process transactions in a timely manner or being unable to resume business in the face of a disaster can all have significant impacts on the effective operation of the business.

Even although the scope of this project was focussed on the IT Service Continuity aspects of BCM – specifically Backup/Recovery, Disaster Recovery, and Enterprise Risk Management – our report includes a recommendation for an overarching BCM program as illustrated in Figure 4.0 below:

Figure 4.0 – BCM Framework

5 KEY ELEMENTS

to be followed for a successful BCM Program



To mitigate the effects of disruption, it is essential the Region prepare and manage a business continuity strategy. A Business Continuity Management (BCM) program will enable the Region to update, control and deploy these plans and align them with their strategic and operational objectives. As the industry leader in BCM, our processes follow the Disaster Recovery Institute (International) framework and best practices guidelines:

Program Initiation

Corporate communication within the Business Continuity Management (BCM) program is the first step to success:

1. Is the Regions BCM strategy clearly aligned with corporate business goals?

2. Have key roles been defined?
3. Framework development

Gaining executive/senior management support & commitment is critical to the success of a Business Continuity Program. Once the Region develops a mission statement/charter for the BCM process, the next step is to define objectives that support the organizations mission. One of the key activities in this stage will be the initiation of a BCM Steering Committee³. This group will provide guidance, oversight, resources, input, and approval throughout the program.

The three main elements of the BCM Program are:

1. Scope – Document what the plan will recover and what it will not – consider the “whole” organizations
2. Objectives – Document what will be delivered at the end of the project & the benefit to the organizations
3. Assumptions – Document all assumptions such as funding & management commitment.

IT Enterprise Risk Management

It all starts with a Risk Assessment and Business Impact Analysis (BIA):

1. Identify organizational risks/threats and vulnerabilities & initiate the BIA
2. Define process Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
3. Automated reporting eliminates the need for cumbersome tools such as spreadsheets.

Risk Evaluation/Control coupled with a Business Impact Analysis will identify threats & vulnerabilities and the likelihood that they will occur – followed by the identification of potential impacts to the business. The result if the analysis is a clear definition of time sensitive processes and the requirements to recover them in a timeframe that’s acceptable to the organizations.

The BCM program must identify the criteria to quantify and qualify impacts such as:

- Customer impact
- Financial Impact
- Regulatory impact
- Reputational impact
- Operational impact

³ The Region could consider leveraging the existing ITS Disaster Recovery Project Steering Committee as a starting point for an overarching BCM program

- Human impact

Strategy and Development

Build a robust business continuity and disaster recovery plan aligned with key industry standards and frameworks:

1. Define operations/technology continuity & recovery strategies
2. Emergency response, Pandemic Preparedness
3. Single, centralized framework

The data collected during the Risk Evaluation and BIA phases can now be used to identify available continuity and recovery strategies for the businesses operations and technology. Recommended strategies must meet RTO and RPO objectives identified in the BIA. A cost benefit analysis is then performed on the recommended strategies to align the cost of implementing the strategy against the assets at risk.

This element also defines Emergency Preparedness and Response requirements to develop and implement the organizations plan for response to emergency situations that may impact safety of employees, visitors, and other assets. Incident Management is introduced which helps you define escalation procedures that help determine criteria for disaster declaration.

Plan Implementation and Documentation

Manage BC/DR & Risk programs and efforts from one, centralized platform:

1. Development of continuity/recovery processes & procedures
2. Crisis/Incident Management fully integrated with dashboards & reports
3. Customized templates

The Business Continuity Plan is a set of documented processes and procedures which will enable the business to continue or recover time sensitive processes to the minimum acceptable level within the timeframe acceptable to the organization. The BCM teams design, develop, and implement the continuity strategies approved by the business and document the recovery plans to be used in response to an incident or event. Our recommended cloud-based system allows you to manage all relevant plans from an easy to access centralized location.

Some of the plans developed during this phase include:

- Disaster Recovery Plans

- Emergency Plan
- Incident Management Plan
- Business Continuity Plan

Plan Implementation and Documentation

Includes a virtual sandbox to test recovery scenarios & perform exercises:

1. Simplify audits and control reviews
2. Crisis communication, awareness & training
3. Plan testing exercises

A program should also be developed and implemented to establish and maintain awareness about the BCM Program and to train staff so they're prepared to respond during an event.

A BCM system allows organizations to perform regular testing from a dedicated recovery sandbox. In order to be effective a BCM Program must implement a regular exercise schedule to establish confidence in the business. As part of the change management program, the tracking and documentation of these activities provides an evaluation of the on-going state of readiness and allows for continuous improvement to recovery capabilities and ensure that plans are complete and accurate.

Recommended Next Steps

Up to 2015 the Region had developed several key pieces in relation to an overarching Business Continuity strategy:

1. A formal IT Disaster Recovery committee was established with key objectives established and tracked
2. Critical IT systems were formally identified as in-scope for Disaster Recovery purposes
3. Disaster Recovery procedures were developed for many applications and systems
4. Testing procedures were developed for some applications and systems
5. A Business Impact Analysis was developed and completed for many applications and systems

Although these activities were carried out up to 2 years ago, much of this work can be leveraged today with updated BCM technology and a refresh of documentation. By following the guidelines outlined in this section of the report, the Region could expect to complete a major portion of this work with 60 – 90 days of effort. Key activities will be:

1. Re-engage the DR Steering Committee and establish revised guidelines and principles as required

2. A formal review of all existing DR documents in order to determine validity and potential requirements to update or remove from the DR plan
3. Procure a BCM cloud solution that will help ensure the success of the program
 - a. The Region can now have a central system to host all corporate activities within the BCM program
4. Identify organizational Risks, Threats and Vulnerabilities
5. Initiate further Business Impact Analysis' "as required" in order to refresh the existing documents
6. Build\Revise DR procedures as required
7. Consider a hosted DR provider
 - a. DRaaS is a cost-effective alternative to procuring hardware\software and managing your own DR site
 - b. The Region can leverage a DRaaS market that has matured and now provides value that was not available 2-3 years ago

Cyber-Insurance

Currently the Region does not hold a Cyber-insurance policy to protect against a data security breach. Generally speaking, any individual or business entity that collects any type of electronic data about people should seriously consider buying Cyber-insurance — it is likely one of the biggest gaps in insurance coverage today. Specific to municipalities, there are common elements in today's policies⁴:

- Crisis management, which may include the expense of investigating an incident and remediating networks;
- Notification, which would cover the cost of notifying all individuals potentially impacted by the loss of data or;
- Municipal loss such as theft of city or regional funds, or fines and penalties assessed.

In addition to this, many insurance companies will not provide cyber-insurance coverage ⁵without a formal Business Continuity Plan. If the coverage is in fact available, the premiums will typically be substantially more than a standard policy for an organization with a formal BCP strategy.

⁴ **Peel Region** - The principal driver in purchasing Cyber-insurance was the broadening of the exclusionary language under CGL with respect to lost data, several incidents of lost data (no claims as of 2017) and the knowledge that in a broad data breach, the cost of managing the breach and the legal fees in dealing with any claims arising therefrom, can be significant, even if ultimately there are no damages paid to those affected by the breach.

⁵ In May of 2017 an Ontario municipality received a letter from their cyber-insurance provider stating "A disaster recovery plan and business continuity plan will be required prior to next renewal in order to continue Cyber Liability coverage".