## VALUE SCORECARD

RATING LEVELS

BUSINESS CONTINUITY MANAGEMENT

LEVEL OF BUSINESS ALIGNMENT

OBSOLESCENCE COST \ EFFORT

IT SERVICE CONTINUITY MANAGEMENT

Packup and Recovery

IT Enterprise Risk Measurement

Disaster Recovery

BCM (ITSCM)

2.1

N/A

CRITICAL (1 - 2.5)

Serious deficiencies have been identified that require attention within the next year

MODERATE (2.6 - 3.5)

Deficiencies discovered that require attention within the next 2 years

PASS (3.6 -5.0)

No deficiencies discovered

BUSINESS CONTINUITY MANAGEMENT (BCM)		
IT Service Continuity Management (ITSCM) — Designed to support the overarching BCM program		
Criteria		ASSESSMENT
LEVEL OF ACCEPTANCE Discipline is accepted by the organization		Backup & Recovery – There are no formal procedures is place although the technology used is considered enterprise-class and adequate Disaster Recovery – There are no formal procedures in place that are currently accepted by the organization IT Enterprise Risk Management – There is no formal program in place to address Risk within ITS
BUSINESS ALIGNMENT Discipline aligns with business objectives		Backup & Recovery – The overall strategy, although informal, is somewhat aligned with the business Disaster Recovery – Some work has been completed and aligned with the business objectives IT Enterprise Risk Management – Nothing has been formalized
OBSOLESCENCE Component is up to date and fully supported		Backup & Recovery – The technology used requires a version upgrade within the next year Disaster Recovery - The work completed in 2015 is outdated and needs to be refreshed IT Enterprise Risk Management – Nothing formal is in place
COST/EFFORT Includes direct costs (HW/SW) and indirect costs downtime/operations)		Backup & Recovery – the solution currently used has a high cost of ownership (high license and operating costs) Disaster Recovery – Replication technology is in place (virtualized work loads) – costs and effort is considered acceptable at this time IT Enterprise Risk Management – Nothing formal is in place

## RECOMMENDATIONS

- Formal procedures and policies need to be developed in all three areas
- A data assessment is required to identify stale unstructured data that should be considered out-of-scope for backup and DR programs
- ¹The Disaster Recovery Program needs to be re-ignited with Business Impact Analysis and Risk Assessments
  - a. Engage the Business Units
- A formal Enterprise Risk Management Program needs to be developed
- Recommend a third-party DRaaS vendor Vandelay should not attempt to manage the DR Program in-house (lack of resources and capabilities)
- Re-engage the DR Steering Committee and establish revised guidelines and principles as required
- A formal review of all existing DR documents in order to determine validity and potential requirements to update or remove from the DR plan
- 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
- Identify organizational Risks, Threats and Vulnerabilities

## 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 policies<sup>2</sup>:

- 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 <sup>3</sup>without 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.

<sup>&</sup>lt;sup>1</sup> 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.

<sup>&</sup>lt;sup>2</sup> Vandelay Competitor - 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.

<sup>&</sup>lt;sup>3</sup> In May of 2017 a competing company 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".