IT Master Plan

Final Report

July 16th, 2018

Perry Group Consulting Ltd.

Version Control

Version	Prepared By	For	Date	Comments
0.1	Gary Walker	D. LucasSwitzer	June 30, 2018	First draft
0.2	Gary Walker	D. LucasSwitzer	July 14, 2018	Second draft
1.0	Gary Walker	D. LucasSwitzer	July 16, 2018	FINAL

Executive Summary

The Importance of Technology

Well run municipalities rely on technology to be effective, to increase the productivity and efficiency of their staff, and to deliver services that satisfy customers with their simplicity.

The Township has clearly recognized the value of this concept with, among other initiatives, a desire to provide faster, easier, and more convenient access to Township services through the delivery of enhanced eServices, the need for collaborative tools in the workplace, and the requirement for the principles, policies, and processes that help define a sound IT governance framework.

All of this points to the importance of technology to the Township. To be effective, the Township must be well equipped and well positioned to implement, manage and leverage technologies to deliver better services to customers – online permitting, digital forms, tax account management online, etc.

Current Situation

So, how is the Township positioned? In developing this strategy, the assessment identified a range of positive aspects, including that:

- The Township has implemented a document/records management solution to address compliancy and data management.
- The Township is leveraging an investment in a Citizens Issues Management solution to enhance the tracking of IT support requests.
- The GIS system is working well as a service delivered/supported by the Counties.
- A substantial investment has been made in a Suez Water Treatment system

However, there were some key gaps and risks to the Township that require attention such as:

- The Township's maturity level with respect to IT security is near zero on most indicators – nothing is formalized and everything is ad hoc.
- An IT Governance framework is non-existent (e.g. steering committee, tactical plans, policies, risk management, etc.).
- There is no formal Business Continuity/Disaster Recovery strategy which puts the Township at risk of severe service outages and data loss.
- The corporate email system lacks key functionality (e.g. shared/integrated calendars) and is currently hosted by a third-party on a single server with no redundancy (this is a major risk).
- There is a significant amount of work ahead around the procurement of new business systems and replacement of existing solutions. This includes the

requirement for solutions pertaining to HRIS, ByLaw Enforcement, Asset Management, Work Orders, and Fire MS. The Township also needs to look at replacing both the Building Inspection and Meeting Agenda solutions, which are currently supported by single individuals respectively. In addition, the Website must be evolved to support online eServices and Vadim[1], following a significant investment, requires vendor support to be further enhanced and evolved.

The findings indicate that there are many opportunities for the Township to improve its ability to leverage technology through strategic partnerships and further investments in IT solutions and services.

Strategic Directions and Key Recommendations

This strategy focuses upon two distinct areas:

1) **Setting the Foundation:** The supporting pillars of the MTA (Municipal Technology Architecture) stack must be in place at the Township as enablers for the upper layers; IT Governance (Strategy, Risk, Business Continuity, Supporting Policies) and Cybersecurity require serious attention and investment as part of the Township's long-term strategy.
2) **Leveraging Technology and Partners as an Enabler of Modern Business Practices**: The Township should implement modern technologies to digitize processes, offer online services and provide staff with tools that simply and enable easy collaboration internally and externally – and leverage partners when it makes "business" sense"

In supporting the recommendations of the strategic directions, the Township should:

1) Set the foundation by:

   a. Implementing IT Governance using the COBIT[2] framework that aligns the IT Strategy with the Business Strategy
   b. Developing a Business Continuity/Disaster Recovery plan that includes a cloud-based recovery service.
   c. Developing core IT policies that address areas such as:
      i. Acceptable Use
      ii. Information Security
      iii. Cloud Computing

[1] Throughout this engagement there have been numerous frustrations with Vadim. The current situation will need an in-depth review in order to determine the ideal roadmap for the Township.

[2] COBIT - (Control Objectives for Information and Related Technologies) is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance.

d. Addressing the security risks outlined in this report and implementing a Cybersecurity strategy

e. Leveraging industry expertise by using out-tasked service providers to manage key areas of technology infrastructure, freeing internal resources to focus on vendor management, and strategic direction.

2) Leverage technology as an enabler of modern business practices by:

a. Digitizing business processes through the implementation of a range of new business systems technologies, including:

   i. Asset and Work Management Systems [3]– effective management of work against assets and mobile technology to enable field crews
   ii. HRIS[4] (cloud) – HR management, employee self service
   iii. Payroll (cloud) – Integration with HRIS
   iv. Website eServices – eSolutions a municipal leader with out of the box capabilities
   v. Fire MS [5]– BeeON software specializes in Fire management systems for smaller municipalities

b. Upgrading/replacing existing systems including:
   i. Council Docs – this solution should be replaced with an enterprise-class eAgenda system that includes webcasting
   ii. ProWare – alternatives should be explored due to the risk involved in utilizing a solution supported by a single individual

c. Modernizing employee experiences
   i. Office365 – Mail / Calendar / Collaboration– modernized, cloud based system
   ii. Mobile Device Management (MDM) – While embracing staff mobility the Township needs to implement an MDM solution to manage the devices.
   iii. Collaboration – enhanced ability to work collaboratively, dealing with documents and web meetings

d. Continue adopting Cloud services and solutions

These recommendations have been detailed in a costed and sequenced work plan which can be found in Section 5 and Appendix E.

---

[3] The purchase of an Asset Management system should be the initial priority over the Work Order system. Once the Township adopts the proper processes they can start to develop a strategy for the selection of a Work Order system (2020).

[4] HRIS (HR Information System) – is a software or online solution for the data entry, data tracking, and data information needs of the Human Resources, payroll, management, and accounting functions within a business.

[5] (MS) - Management System to manage the daily operations and reporting requirements for Fire Departments.

Conclusion

To be successful with this Strategy, the Township needs to first address the core foundational requirements, focusing on the priorities identified within this strategy. This will require investment in IT at suitable levels to meet the needs of staff, compliancy, and the expectations of customers.

The Township should make technology more central to the way it thinks and approaches business challenges, opportunities and improvements. The recommendations in this Strategy will help drive technology improvements into all business areas – meeting the evolving needs of customers and stakeholders.

As the fastest growing community in the region, the Township's investment in IT governance and technology will ensure its place as a leader in innovation and transformation.

Table of Contents

Executive Summary **3**
The Importance of Technology 3
Current Situation 3
Strategic Directions and Key Recommendations 4
Conclusion 6

Table of Contents **7**

1. Introduction **8**
1.1 The Importance of Technology for the Township 8
1.2 The Role of Technology and IT Governance in Supporting Growth 9
1.3 Importance of the IT Master Plan (ITMP) 10
1.4 How the ITMP was Developed 11

2. Findings **12**
2.1 Technology Systems 12
2.2 IT Management Practices 19
2.3 Key Issues for the Township to Address 21

3. The Strategy **23**
3.1 Elevate the Importance of Technology Management Frameworks 23
3.2 Use Technology & Strong Partnerships to drive Modernization of Business Practices 33
3.3 Summary 38

4. Major Initiatives **39**
4.1 Major Infrastructure Projects 39
4.2 Major Business Solutions 42
4.3 Integration 44
4.4 Customer Facing Solutions 45

5. Implementation Plan and Budget Implications **46**
5.1 Major Initiatives – 2018 Task List 46
5.2 Additional Considerations 47
5.3 Budget Summary Estimate (by year) 48

Appendix A – Security, Operations, & Data Management Scorecards **49**

Appendix B – Current State Infrastructure **53**

Appendix C – Potential Future Infrastructure (Phase 1) **54**

Appendix D – IT Service Continuity Management **55**

Appendix E – Workplan **56**

Appendix F – Mobile Device Management Options **58**

Appendix G – Township of South Stormont 2018 Task List (Expanded) **59**

1. Introduction

1.1 The Importance of Technology for the Township

The best run municipalities around the world, large and small, rely on technology to be effective, to increase the productivity and efficiency of their staff - delivering services and continuous improvement to its customers.

Just as maintaining a healthy infrastructure of water delivery and roads is essential to the functioning of cities and townships, a healthy infrastructure of information technology has also become a critical component in the support of municipal trends in open data, online citizen engagement, and community dashboards. Deterioration in IT infrastructure can lead to deterioration in production and service delivery. While this is self-evident to IT professionals, it may not be as obvious to senior management.

Currently, the Township relies upon the Counties to host core financial system technology in the back office, and various third-party providers to support services such as email, building inspection, water treatment management, citizen issue tracking, and recreation management. Ancillary support solutions for file management, helpdesk, and network services are supported in-house (level 1) with additional support provided by the Counties (level 2).

While the Township has made some progress in some areas, looking to the future, technology will only continue to grow in importance.

Existing systems reaching end of life must be replaced, as will those providing inadequate functionality. New systems will be required by the Township to address emerging needs such as HRIS, Payroll, Asset Management, eServices, Fire MS, By-Law Enforcement and Work Order Management.

Given the importance of information technology to all functions of the Township, Senior Management, with the support of Council, must be strong advocates for appropriate life-cycle processes for IT infrastructure. One responsibility of IT is to provide executive staff with appropriate background, analysis, and recommendations about IT infrastructure, focusing on the impact that inappropriately maintained or out-of-date IT infrastructure may have on the various functions of the corporation.

As we continue to move forward, more customers will expect to use their computers, smartphones to interact with the Township. The Township will increasingly employ what are referred to as smart technologies and be more connected as Township-wide sensors are used to monitor critical infrastructure and alert staff to where problems are anticipated or have occurred. Data, information, and the supporting infrastructure will become more important, providing insights about service delivery that allow Township officials to optimize efficiency and improve services.

Therefore, the Township needs to be well positioned to implement and manage technologies that are increasingly becoming central to its effectiveness.

1.2 The Role of Technology and IT Governance in Supporting Growth

As requirements to deliver enhanced services continues to grow, technology has a pivotal role to play within the Township – be it across departments, or from front to back office. Using common, integrated systems ensures that inquiries flow from front counters to the back office and to appropriate field staff for resolution. Various technologies support the no wrong door approach – allowing customers to choose their channel of choice with which to interact with the Township. Common systems allow a consistent view of the customer for customer service agents and allow for simple dashboards and data analytics to support Management and Council in the monitoring and oversight of service quality.

However, equally important will be the operational elements that encompass IT Governance; Leveraging frameworks such as COBIT[6] and ITIL[7] will be critical for the Township.

From the perspective of the IT users within an organization, IT governance is often seen as an unnecessary set of procedures set by senior management that hinders the productivity of the organization. While IT governance does represent a set of management standards and policies to be followed, at its core IT governance is primarily concerned with the alignment of the goals and objectives of the business with the utilization of its IT resources to effectively achieve the desired results. The end result of good IT governance is that it aligns your business strategically to support the growth of the IT enterprise architecture so that it delivers consistent and improved business value. In contrast, poor IT governance can lead to wasted resource efforts and expose an organization to IT security and service availability risks.

Does moving to the Cloud limit the need for IT Governance?

This question is often asked, and the answer is unequivocally "No". Cloud computing requires governance. Which is to say that cloud computing needs processes, policies, and procedures. In a way, this is no different from IT more broadly. But virtualization, dynamically moving workloads, and an increased reliance on third parties for many types of IT functions mean that well thought-out and documented processes, policies, and procedures tend to be more important in cloud computing than with a more static and manual environment.

[6] **COBIT (Control Objectives for Information and Related Technology)** - an IT governance framework and supporting toolset that allows organizations to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice, emphasizing regulatory compliance, increasing the value attained from IT.

[7] **ITIL (Information Technology Infrastructure Library)** - is a framework that provides a set of detailed practices for IT service management (ITSM) with a focus on aligning IT services with the needs of business.

The Township will face a series of pressures as it grows, that technology and governance should assist with:

Some existing practices will not scale. As the demand for digital information and data exchange grows, it simply becomes impossible for paper and personal knowledge-based processes to be effective at coordinating activities both internally and external to the organization. To support these requirements, existing knowledge, processes and procedures must be captured and digitized into integrated systems. This helps new staff easily adopt Township processes, ensures the knowledge of long standing employees can be captured for succession planning purposes.

Technology demand means increasing complexity. The implementation of new systems does not come without its challenges. The complexity in supporting and managing these new systems will also grow - whether they be internal systems or cloud services. Accordingly, the importance of integrated planning and governance across departments and agencies will grow.

Pressure on core services. All departments are reliant on core corporate services, but HR and Financial processes in particular are critical business processes in discharging their responsibilities. Eliminating manual processes, product challenges, and potential performance issues that inhibit Township departments' ability to move at the speed they need, can all be achieved using technology and adopting sound IT governance.

1.3 Importance of the IT Master Plan (ITMP)

Therefore, given the ever-increasing importance of technology and governance and their roles in delivering municipal services, the ITMP is a crucial piece of work. Amongst the many opportunities identified during the course of this engagement, the ITMP must help the Township determine its priorities and identify the key initiatives and activities that will support its goals and objectives.

It allows the Township to ask questions which are central to future success:

- Is the Information Technology environment properly managed, maintained, secured, and able to support the needs of the Township?
- Is the IT service cost effective?
- Is there a sound governance model in place?
- Is the technology environment, resources and management practices equipped to meet current and future business needs?

It's important to note that this ITMP also included a security assessment that involved the installation of a security appliance which was used to monitor network activity within the Township's Municipal Office in Long Sault. The results of this analysis can be found in **Appendix A.**

1.4 How the ITMP was Developed

The project to develop the ITMP was approached in two main phases: Discovery & Recommendations.

The Discovery phase kicked off in April 2018, with a set of on-site interviews, meetings, and assessments (technical and non-technical) involving staff, vendors, and management. At the conclusion of the discovery phase initial findings and observations were shared with the Town's project leads (CAO and Director of Corporate Services).

As part of the Recommendations phase we conducted an onsite working session with the CAO and Director of Corporate Services to establish important strategic directions on topics such as technology, governance and business systems. We also worked collaboratively with Township vendors, using this output to define the optimal future approach to technology, roles and responsibilities and governance.

The strategic direction was then translated into a set of costed initiatives, a proposed list of priorities, with recommendations developed and reviewed. This final report compiles the results of both phases and was delivered in July 2018.

2. Findings

An assessment of the current state was the starting point for developing the strategy. To review the current state, the consulting team looked at various aspects of technology and technology management, including 1) Technology Systems, and 2) IT Management Practices. The following section provides a high-level summary of the results of the findings.

2.1 Technology Systems

2.1.1 Introducing the Municipal Technology Architecture

Perry Group's Municipal Technology Architecture (MTA) is shown in Figure 1 below.

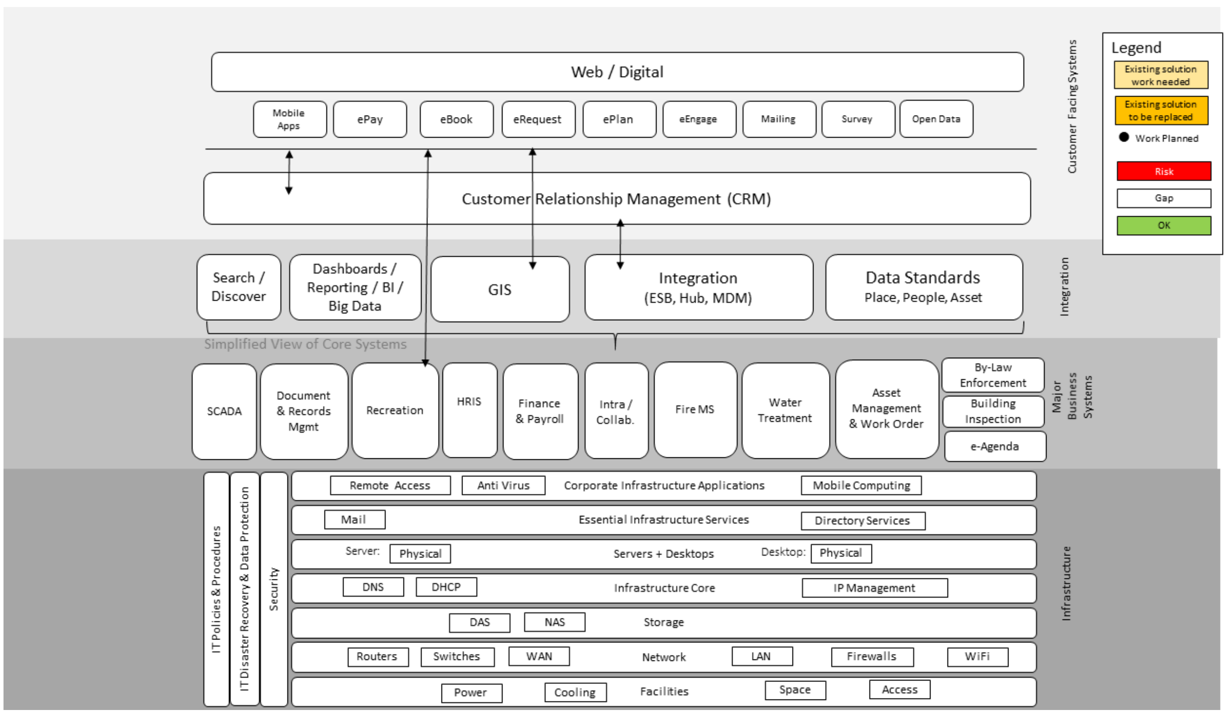


Figure 1: Municipal Technology Architecture

This is a conceptual municipal IT model that has been developed and refined by Perry Group in consultation with many municipalities over the past 10 years. The MTA identifies the technologies that a municipality should have in place, and provides a framework for the consulting team to assess a municipality's technology environment.

The MTA introduces several key concepts that are important for the Township:

- There are 4 main technology layers (labeled in Figure 1 as: infrastructure, business systems, integration, customer facing). Each requires discrete IT skill sets to be managed effectively. For instance, while technology infrastructure management is deeply technical, business systems projects require project and process management, change management and people skills. Web projects need development and UX (User Experience) expertise. An IT organization needs a breadth of skills, across the various layers to effectively manage the complete environment.

- The Infrastructure layer is the foundation for the entire technology environment. Infrastructure must be robust and reliable because it provides the foundations for all other layers. Unreliable infrastructure undermines all the technology that sits above it.

- Appropriate policies, security, data protection and disaster recovery provisions should be in place to protect the Township's information assets and meet its legal compliance obligations. Ideally, the IT team should have the tools needed to help manage the environment efficiently. These include a helpdesk request tracking system, systems management solutions, and automation tools (e.g. remote support, patch management, mobile device management) to simplify IT management tasks, increase IT staff productivity and enable employee self-service (e.g. password resets).

- A municipality should limit the number of corporate business system platforms it runs to minimize process and information silos. These core systems should be purchased off-the shelf solutions configured to support the Township's business processes – customization should be avoided. These business systems, or business platforms will provide the foundations for automated and streamlined business processes. They will gather data to drive analytics capabilities and underpin the effective delivery of online services.

- Business systems should be integrated allowing for data to be automatically passed between systems (using integration technologies), thus reducing data duplication and errors, and ensuring auditability, whilst enabling data analysis and predictive capabilities.

- Customer facing digital solutions should allow customers to easily find information and answers to common questions, to transact with the Township, submitting requests and applications, making payments, and allow the Township to engage with Citizens to seek their input on important decisions. All of these systems must be integrated into back office systems – if processes are not digitized in the back office, they cannot effectively be offered online.

- The IT architecture should build from the bottom up – Infrastructure first, then business systems and so on.

These are some of the basic tenets that underpin a well-designed municipal technology environment.

2.1.2 Assessing the Township's Technology against the MTA

At the conclusion of the Discovery phase, a detailed findings report was prepared and shared with the CAO and Director of Corporate Services.

Figure 2 provides a visual summary of the results of the consultant's assessment.

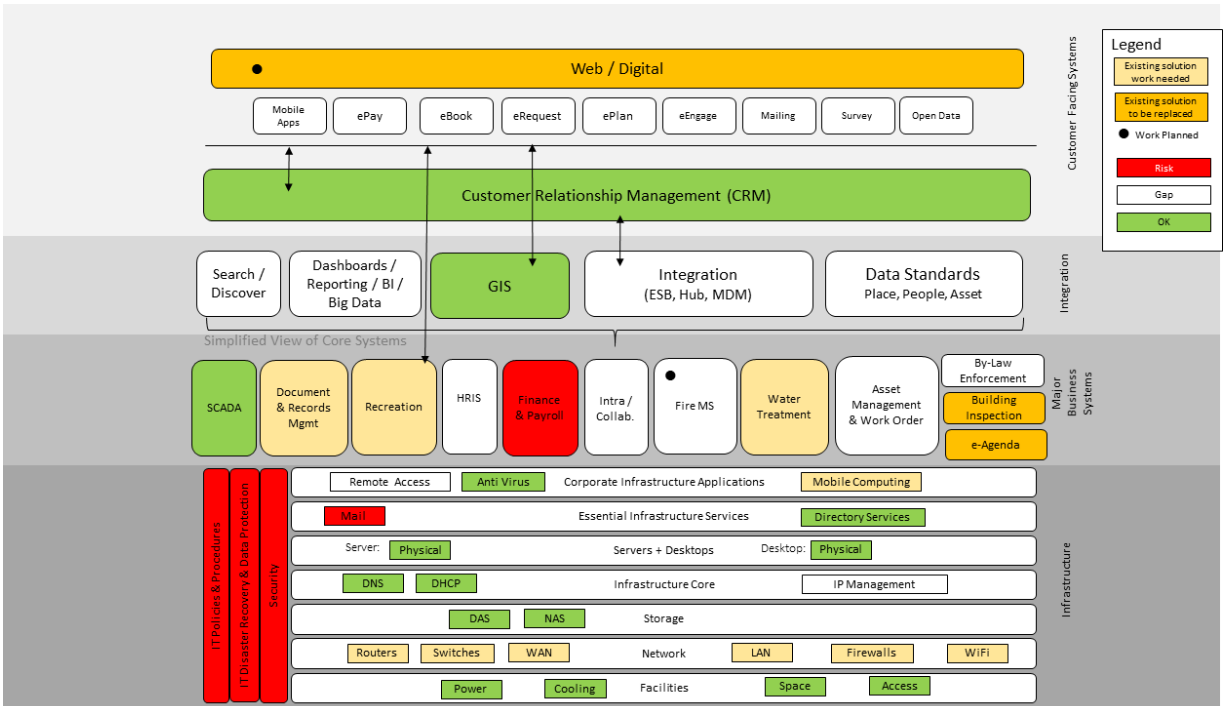


Figure 2: MTA Assessment Results

The following section highlights key points in each layer of the MTA.

Infrastructure (General)

Positive aspects:

- There are standards around hardware procurement
- The infrastructure seems to be reliable
- There is a records/document management system in place
  - The Township follows Tom RMS for records management
- A third-party solution for citizen issues (AccessE11) is being leveraged to log IT helpdesk tickets

Key Issues:

- The Township is not following a formal **IT Governance** framework. As such, there are no formal processes, policies or procedures pertaining to the management of IT
- There is no **Business Continuity/Disaster Recovery** Plan in place – this has exposed the Township to the possibility of extensive service outages in the event of system interruptions or disasters
- **Mobile Computing** – there is no strategy to define how mobile devices will managed. In the age of mobile computing this is an important component for most organizations
- There is no formal **Cloud Strategy** in place - As the Township moves forward, cloud services will underpin the delivery of new digital business innovations. A cloud strategy clearly defines the business outcomes an organization seeks and how you will get there
- The current **Email Service** (Ignit) does not provide enterprise-class functionality and system redundancy. This has resulted in inefficiencies and a risk of an major outage to a core business function (email). There is also a large amount of SPAM email that gets through to Township staff due to a lack of proper filtering from the current provider
- **Lack of Connectivity** (e.g. Arena) – As it stands connectivity from the 9 ancillary locations identified does not exist. In some cases Township staff must drive from remote locations to the municipal office to complete processes.
- **Poor Connectivity** to the Counties over MPLS connection to Vadim systems (1Mbps/10Mbps). This is a slow connection by todays standards and might be contributing to the issues accessing this system
- **Backup Procedures** have not been formally developed which has resulted in a risk of data loss and data breach. It was also highlighted that there may be external hard drives and USB memory sticks in use with Township data that are not being backed up or secured.
- There are no **Remote Access** capabilities available to any of the Township's core business systems
- There are no **Document Collaboration/Knowledgebase Systems** are in place. Like most work environments, the Township would benefit having tools enabling employees to collaborate with colleagues effectively, producing a more educated, skilled and engaged workforce.

Infrastructure (Security)

The security audit performed identified that historically the Township has had a "best effort" approach to IT security focusing on traditional IT operational tasks to deliver quality services as perceived by their users.

Security has always been addressed with an ad hoc approach based on timelines, budgets and available resources. Generally speaking, nothing is formalized and documented, and the quality of the services being delivered relies on the qualified staff and their dedication to the Township.

Evaluating the actual maturity of an IT group that does not document and formalize any of the core security elements remains difficult and we have provided our professional opinion on the overall maturity of the current ecosystem making sure to provide the insight required to explain the rating applied.

Each area reviewed includes a description of the observations, along with a list of “next steps” and a list of the questions you should be able to answer once you have optimized the subject at hand.

Management should keep in mind that the scores are low because very little is formalized, documented or provable and it is apparent that security was never prioritized in the past. This means that any investment in the areas evaluated will translate into a much better scoring in the future.

It is important to note that this evaluation is a high level evaluation, as budget constraints did not permit a full audit. However, the observations documented in this report remain accurate. It is also important to highlight the following key observations:

1. Currently, the reliance on the IT staff is critical. Any changes to that ecosystem will have significant impacts across security.
2. No formal security role is in place, and this responsibility is a requirement going forward in order to continuously optimize security.
3. KPI’s are needed that will be presented to management periodically. Periodic assessments are a primary means of identifying significant weaknesses before a malicious actor exploits them.

Positive aspects:

- There has been minimal issues up to this point but this should be considered as extremely fortunate for the Township when we consider the issues/gaps

Key Issues

- From an over all **IT Security Maturity** point of view, the Township is near zero on most indicators
- Almost everything analyzed is near zero as **Nothing is Formalized** and everything is ad-hoc
- Some patching and configuration optimization is required from the **Vulnerability Testing Results**
- **No Official Hardening** (configuration) standards are in place (servers and workstations need optimization)
- **User Password Policy** is extremely weak with many users having extremely poor passwords – some using only “two” alphanumeric characters.
- **No Cyber Insurance** is in place to protect the Township for data breaches. These incidents can have a considerable financial impact on a public entity, including the cost of lawsuits, crisis management and notification of the affected parties.

Full the full report please refer to supplementary document **“South Stormont Security Assessment Report – Logicnet”**

Business Systems

Positives:

- The Township has made some investments in systems that are being used by other municipalities, allowing for the exchange of knowledge.
- **FileHold** was implemented in 2015 as a electronic content management system. This solution appears to be working well, although scheduled training sessions would help the Township further leverage the capabilities of the solution

Key Issues:

- **Vadim (iCity)** – Users are extremely frustrated with this system. The issues appear to be a combination of poor vendor support, product functionality, and the configuration of the delivery mechanism from the Counties.
- Although the scheduling component of **BookKing** works well, there is no Vadim integration for the financials (although it is supposed to be available). This has resulted in an inefficient (insecure) process using spreadsheets and manual workarounds
- **Payroll** is currently a manual process
- There is no **HRIS System** in place
- There no solution in place to track and manage the **Township's Municipal Assets**
- There is no system in place to track the progress and completion of **Work Orders**
- There is currently no **Management System** for **Fire**
- **Council Docs** software needs to be replaced as it lacks functionality (e.g. Webcasting) and support
- The solution being used for **Building Inspection (Proware)** has been developed and is supported by a single individual. This has created issues in getting product enhancements
- The Township needs to understand/unlock **AccessE11** capabilities (including By-Law Enforcement functionality)
- There are too many manual work-arounds outside of the systems and /or point solutions being used

Integration

Positives:

- GIS is widely acknowledged as a high value system across organization
- The agreement with the Counties (GIS) appears to be working well

Key Issues:

- There is currently very limited integration between systems

Customer Facing

Positives:

- The cloud-based Citizen Relationship Management system is working well (AccessE11)
- The website offers some limited eServices
  - Recreation program registration
  - VadimOpen is used to allow customers to view property taxes and water and sewer (utility) billing

Key Issues:

- **Website** lacks many eServices capabilities (e.g. dog tags, marriage certs, etc.)
- Absence of a **Service Delivery** strategy or roadmap
- The Website is in need of a major refresh / update
- There is very **Limited Interactive / Intelligent Forms**
- There are limited opportunities to pay, book, report online
- Limited end-to-end services
- Overall, the Township is lacking technology components to support digital delivery – eForms, Payments, Signatures, etc.

Summary

In summary, the assessment indicates that there is significant work needed in all layers of the MTA

- There are some good positives in the infrastructure layer, with a series of 'green' rated elements. However, there are some key areas that must be addressed such as:
  - IT Policies and Procedures (IT Governance)
  - Business Continuity/Disaster Recovery
  - Security Risks
  - Email Service Risks
  - Mobile Device Management
- A significant amount of work is also ahead in the Business Solutions Layer to either procure new systems or replace/upgrade existing solutions including:
  - New system requirements – HRIS, Payroll, Asset Management, Work Orders. Fire MS, By-law
  - Replacement of Council Docs solution
  - Investigate the potential replacement of Proware (building inspection)
  - Fix issues/concerns with Vadim
- Although there has been some good work around the GIS, there has been very limited progress to date at the integration level. This is understandable because integration depends on the business systems and there remains significant work in that area before work on integration should proceed too far.
- Major work is needed at the Customer facing level, specifically in respects to the development of eServices on the website – but note that much of the work to offer digital services to customers is dependent upon the digitization of back office work processes and the development of a corporate customer service strategy.

Figure 3 illustrates the total ratings for all areas assessed as part of the overall infrastructure health check (IHC). This rating (1-5) can be used as a baseline for future assessments, allowing the Township to monitoring trends in the respective areas.

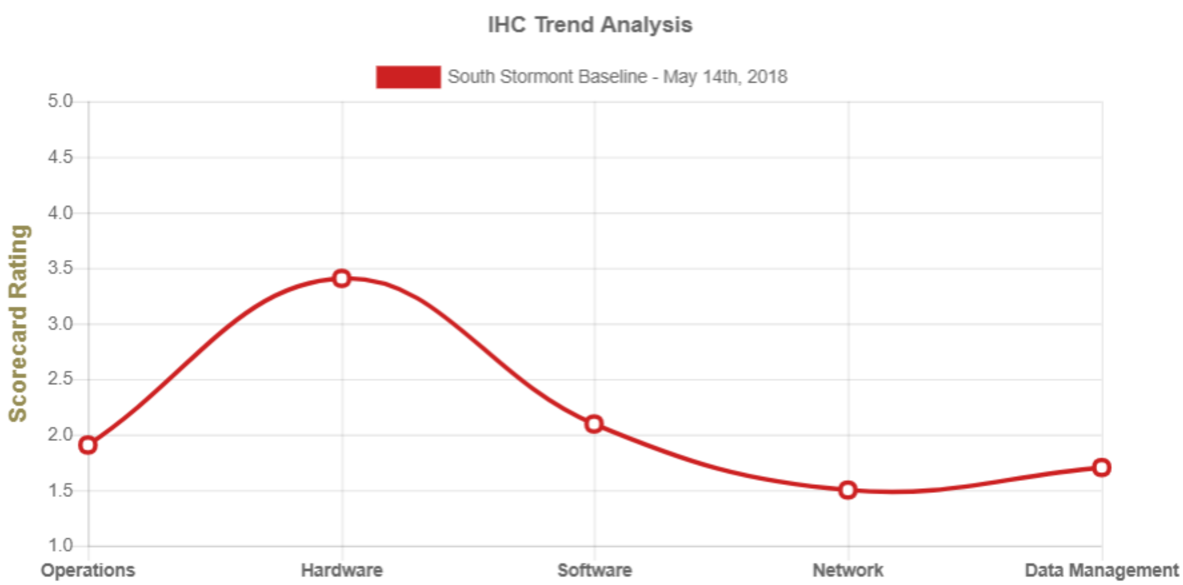


Figure 3: Township of South Stormont Trend Analysis Graph

2.2 IT Management Practices

Figure 4 identifies the Township's rating levels in the respective areas of the assessment. As can be seen, the Township has, at the point of our assessment, very little best practice processes in place for effective management of IT.

This is quite common in smaller municipalities that struggle to manage technology.

Technology changes rapidly, and businesses need to keep up with technological advances to ensure the tools they are using are effective and conducive to productivity. However, at the same time, keeping up with technological advances can be expensive, especially for smaller organizations.

IT Management	
	Rating Level
Governance	1.4
Financial Management	1.3
Project and Program Management	2.0
Architecture and Roadmaps	1.4
IT Organization	2.5
Business Systems	1.7
Technology Infrastructure	2.0
Data Management	2.5
Business Continuity Management	1.0
Procurement	3.0
Training	2.5
IT Service Management	2.0
IT Security	2.0

Figure 4: Township of South Stormont Scorecard: Governance Groups and Processes Ratings 1(lowest) – 5 (highest)

2.2.1 IT Governance

IT governance is the broad term given to the groups, processes and methods that are used to make effective technology decisions – how IT decisions are made. Effective IT governance is essential if an organization is to control, coordinate and ultimately derive the best value from its investments in technology.

More generally speaking, there has been a lack of organizational understanding about what it takes to deliver successful technology solutions and a tendency to under-estimate project costs and the resources required to deliver the project to secure budget approval. This starts projects on a poor footing, from which it is almost impossible to recover.

Some key areas requiring attention include:

- IT Governance Framework – there is no overarching framework that assigned appropriate decision making to the right groups
- Executive Level IT Steering Committee – there is nothing in place at this time
- IT Policies – there are very limited policies in place at this time
- IT Risk Management – there is no risk management framework in place at this time

2.2.2 IT Resourcing

The Township currently employs a contract resource to manage level 1 support. Issues that require additional technical expertise (L2/3) are escalated to either the Counties or appropriate vendor depending on the issue.

Despite the arrangement with the Counties, the there are clear gaps:

- There is a lack of technology staff (Township & Counties) to support the technology infrastructure and provide proper strategic planning – this is clearly evident with respect to ongoing issues with the delivery of Vadim services from the Counties
- There does not appear to be a formal service catalogue outlining what the Counties provides, and does not provide, for the Township
- Due to the size of the Township, there is a lack of business solutions support (Applications Analysts) in support of important systems (this includes staff and vendors). With a municipality of this size, support from either the upper tier (Counties) or solution vendors becomes critical.
- Because of this situation, staff are quite often required to fulfill roles that are not part of the job description – pulling them away from other work that is needed

When working with the third-party for IT support, a well defined IT support model is essential.

2.3 Key Issues for the Township to Address

There are a number of positives from which to build:

- New Township leadership (CAO) has led to increased attention, focus and investment in information technology – this will lead to a substantial improvement in services
- Corporate Services leadership has embraced the new direction
- New IT leadership at the Counties has proven to provide a fresh outlook on support and overall approach to IT strategy
- There has been a clear acknowledgement of the importance of the IT Master Plan
- Good skills and capabilities within the business units will help drive the plan

Nonetheless, there are clearly some key issues to address if the Township is to maximize the value it can get from technology. The consulting team identified the following priority areas of focus for the Township:

- The Township needs to develop core IT policies that address key areas such as acceptable use of Township assets, password requirements, security, cloud computing, etc. as part of an over-arching IT Governance strategy

- The issues outlined in the security assessment need to be addressed, leading into a more formalized approach to IT security.
- A Business Continuity/Disaster Recovery strategy needs to be developed and managed as a “program”. This process should include formal business impact analyses and risk assessments to develop Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for core Township processes.
- If the Counties is to continue providing support for the Township, there must be a more formalized IT Service Management (ITSM) process/framework developed (e.g. ITIL). This should also include a roadmap that defines the Counties plans to improve service delivery as part of Continual Service Improvements (CSI)
- A significant amount of work is ahead in the Business Solutions Layer. Business solutions that the Township has is earmarked either for replacement or significant work include procurement of HRIS, Payroll, Asset Management, Work Order, Bylaw, eAgenda, systems. In addition, existing systems such as Vadim must be evolved to support the business and mobile working.
- The organization is lacking maturity in its approach to business-technology initiatives, which leads to under-planning, under-estimating and under-resourcing technology initiatives – which set them up for failure. The Township needs to better control which projects is chooses to invest in and how projects are to be undertaken

Please refer to Appendix B for an overview of the Current State Infrastructure

3. The Strategy

The strategy introduces two key areas of focus:

1) **Elevate the Importance of Technology Management Frameworks**
2) **Use Technology & Strong Partnerships to drive Modernization of Business Practices**

3.1 Elevate the Importance of Technology Management Frameworks

One of the primary goals of the ITMP is to create a framework that establishes the conditions for future, ongoing and sustained success with technology. Thus, many of the primary recommendations within the strategy are focused on how to approach technology and how technology is to be managed. Examples used in this report have been COBIT (IT Governance) and ITIL (IT Service Management). Other *supporting* frameworks can/should be followed from cybersecurity organizations such as NIST (National Institute of Standards and Technology) or ISO (International Standards Organization).

When we consider the size of the Township, the goal should be to leverage third-party security expertise and ensure that strategic partners (*i.e. vendors, SDG Counties, other local municipalities*) are following similar guidelines[8]. This should also be the case in the areas of IT Governance and IT Service Management.

As the Township continues to transition from one cloud provider to a multi cloud consumption model, the importance of governance increases several-fold.

The **Security Assessment** recommendations highlighted several areas that needed attention. Based on these results, this strategy will focus on the need for key frameworks in the following three areas:

1. IT Governance (COBIT)
2. IT Security (NIST)
3. IT Service Management (ITIL)

[8] **What Cybersecurity Framework Is Recommended?** If you ask an IT security professional to identify their preferred best practice, it generally comes down to NIST or ISO. If you look at this from the perspective of a debate over which soft drink tastes best (e.g., Coke vs Pepsi), it comes down to personal preferences, since both products are essentially sugary, carbonated drinks and only differ slightly in flavor and packaging. The same arguments can be made for IT security's two heavy hitters – NIST and ISO. These frameworks both cover the same fundamental building blocks of an IT security program but differ in some content and layout. Both can be great solutions and may organization leverage both along with other frameworks. The Township's security advisor should/will provide guidance.

3.1.1 IT Governance (COBIT)

One of the most important areas of work for the Township is to establish a formalized Governance for Enterprise IT (GEIT) framework to allocate technology decision making rights appropriately, ensuring that decisions and resources are suitably aligned with corporate goals.

For the Township, IT Governance, and specifically COBIT(5), represents and provides a way to maximize value from investments in IT. The primary focus of IT Governance in COBIT 5 is value creation, achieved by realizing benefits, and optimizing risks and resources. The IT function of the stereotypical small municipality ranges from a small team down to a 'one-person-band' where the IT resource(s) perform many other tasks of which but one is related to IT. IT tasks tend to be very technically oriented with little evidence of management or governance in place.

Without dedicated IT Management and often not even an IT Help Desk in place, small municipalities are commonly at a disadvantage when contemplating how to go about investing, managing and governing their Enterprise IT. Many are not even aware of IT Governance or frameworks and how it can be used to improve IT business performance, and are rather reputed for poor IT spends, security, resource and risk management, even in the age of globalization and the information (and technology) economy.

So many still today believe that IT Governance and COBIT 5 are the domain of 'big business', reserved for the large enterprise sector and not available, affordable and practical for the smaller organization.

Fortunately this is not the case, as emphasized in the ITMP.

Many of the benefits which can be realized by the Township from its Enterprise IT, are a result of organizational size - as opposed to it being a barrier – like flexibility, adaptability, responsiveness, competitive advantage. Smaller municipalities find it difficult to set IT Goals, implement IT processes and practices, and measure their IT performance, and again this is where IT Governance and the COBIT 5 business framework are able to help.

The following areas should be tackled first as an initial entry point into IT Governance for the Township:

1. IT Steering Committee
2. IT Policies
3. IT Risk Management

IT Steering Committee

An IT Steering Committee is an administrative body that reviews, monitors and prioritizes major IT projects from a cross-functional perspective. The two key concerns of a technology steering committee are:

1. **Alignment.** The committee helps ensure that IT strategy is aligned with the strategic goals of the organization.

2. **Ownership.** The business units represented on the steering committee have ultimate ownership over the larger IT strategic decisions since those decisions will impact their processes.

The top three activities of IT steering committees are IT project prioritization, approval of IT projects, and IT strategic planning. Organizations that operate effective IT steering committees realize better IT project priority setting as well as improved alignment with business objectives.

An IT steering committee brings a number of benefits to both the IT leader and the enterprise as a whole:

- **Business focus.** The IT steering committee's strongest mandate is to find & align business solutions that may leverage technology.

- **Priority.** At budget time, IT will be able to set spending priorities according to broadly based business recommendations.

- **Transparency.** Other departments will be able to see their IT demands in the larger context of strategic plans, and at least understand (though maybe not agree with) the rationale behind decisions to proceed with one project over another.

- **Accountability.** IT projects, especially cross functional projects will be decided upon based on committee approval and priority and not just within the IT business unit.

Considering the size of the Township, the IT Steering committee can include trusted "advisors" such as:

1. Peers - Other municipalities or even local businesses
2. Strategic Partners – This could be a vendor that's able to provide objective advice on technology decisions such as a member of PGC

IT Policies

Developing an IT policy framework from scratch can be a very daunting challenge for even the most experienced professionals. It is not uncommon to find even larger companies lacking an IT framework and policies.

For simplicity, IT Policies should be broken down into the following categories:

1. IT Governance, Risk and Compliance policies.
2. Project and Change Management policies.
3. IT Procurement policies.
4. Service Availability policies, like disaster recovery (DR), business continuity (BC).
5. Acceptable Use policies, like an email usage policy or computer usage policy.

6. Information Security policies - focus on managing and protecting and preserving information (including personal information) belonging to the organization, which is generated by those employees in the course and scope of their employment.
7. Information Management policies - focus on managing data such as its retention and destruction.

We recommend a draft or review of IT policies through a “legal lens” focusing on legal compliance and legal risk issues in accordance with a well-defined Policy Framework. In addition, the development of IT policies should also include a review of existing policies that may require cross-referencing and alignment.

Issue and audience

There are two key questions relating to any policy:

1. What is the issue to be addressed?
2. Who is the intended audience? Who must comply with the policy?

Issue-specific IT policies

There are many essential issue-specific policies such as:

1. Access control
2. Acceptable Use of IT
3. Use of Software
4. Protection from Malicious Software
5. Bring your own device (BYOD) or personally owned devices
6. Mobility use and management
7. Telecommuting
8. Computer use
9. Email use
10. Incident response
11. Internet use
12. Mobile technology
13. Monitoring or interception of communications
14. Physical and environmental security
15. User accounts and passwords
16. Backing up of information
17. External facing and internal facing privacy policies
18. Protection of Personal Information Policy or Data Protection Policy
19. Social media
20. Email archiving policies

Combined IT Policy

We recommend an approach which clearly differentiates between issue-specific, operational policies, standards and procedures, each of which should be set forth in separate documents. However, one policy that covers several areas of acceptable use can be created in a combined document e.g. Acceptable Use of IT Policy. It is essentially several specific policies wrapped into one document directed at one intended audience (e.g. users).

Characteristics of Good Policies
They should be:

- short and to the point
- in plain and understandable language
- well structured
- consistent
- in accordance with and inline with the latest laws and rules
- clear on what is permitted and what is not
- specific, relevant and applicable to the target audience

Policy Framework

There is no security policy standard and no general consensus as to what policies or how many should be in place, nor is there general consensus on policy design or content. Some organizations have a single generic document which combines policy, guidelines and standards (the combination approach), while others have multiple policies, guidelines and standards documents.

We recommend an approach for the Township which clearly differentiates between issue specific, operational policies, standards and procedures, each of which should be set forth in separate documents. The need to clearly differentiate between them is emphasised by the ISO 9000 Quality Standards for the preparation of internal documentation. For example, these ISO standards expressly state that policies must be separate and distinct from procedures.

Policies that are successfully implemented:

1. follow a document hierarchy;
2. take into account the organization's own identified risks and business needs;
3. put in place a set of information security measures to demonstrate that the organization exercised due care and was not negligent;
4. are compatible with the organization's culture and are thus more likely to be accepted and supported;
5. are aimed at different audiences; and
6. are kept up to date.

Document hierarchy
Typically, such a framework would include a document hierarchy that includes the following:

- **Charter: (or mission statement)** a concise document positioned at the top of the hierarchy that forms the capstone of the policies and presents the organization's philosophy of information security and establishes a management mandate for and commitment to implementing that philosophy;

- **Policies:** There should be issue specific, operational policies that apply to specific issues (see the types of policies) and domains (for example applications, business units and regions) that must be complied with by all persons accessing these domains and to whom the issues apply;
- **Standards:** these specify mandatory, uniform uses of specific technologies, configurations and procedures;
- **Procedures:** provide detailed steps (sometimes in the form of a checklist) to be followed to achieve a particular recurring task (for example assigning appropriate privileges, running daily backups and updating firewall rules);
- **Guidelines:** provide additional (optional) advice and support for policies, standards and procedures, as well as general guidance on issues such as how to secure systems, what to do in particular circumstances etc.

Audience-driven approach

Generally, policies are directed at several significantly different audiences because each audience has distinctly different needs.

For example, with end users, the focus is generally on acceptable use. But who is an end user? Is it permanent employees only or does it include people on fixed term contracts? What about suppliers?

With technical staff the focus is in much more detail, such as how to carry out the monitoring of a user email inbox or how to respond to a security incident or privacy breach. Separate documents should therefore be addressed to separate audiences so that the relevant audience is provided with only the information that is relevant to them. People need to only read those policies that directly apply to their own job.

Some policies are also directed at customers or management.

Characteristics of good policies

Generally, issue-specific policies are easy to read, easy to rely on, easy to implement, easy to manage, easy to implement and easy to rely on in a court of law:

- **Easy to read:** In the fast-paced information economy in which we live, people are pressed for time and will generally only read things that are relevant to them. The policies should therefore be in plain language and focused on particular audiences (typically end users, management and technical staff) addressing only those issues that are absolutely needed and that focus only on the essentials. Addressing a policy to multiple categories on readers makes it hard for the reader to find relevant information. For example, they might have to sift through a whole lot of rules before getting to the relevant rule relating to their email use.
- **Easy to rely on:** With issue specific policies, it is easy accompany those policies with necessary guidelines or standards or procedures.

- **Easy to manage:** Problems that arise tend to relate to issues and if those problems are recorded on an issue by issue basis, then it is easier to update the issue specific policies when reviewed annually.
- **Easy to implement:** For purposes of education and awareness, issue-specific policies make it easier to convey key messages throughout the organization.
- **Easy to rely on in a court of law:** One of the essential guidelines in cases of dismissal for misconduct for determining whether a dismissal or misconduct is unfair is whether or not the employee contravened a rule or standard regulating conduct … the rule was a valid or reasonable rule or standard … the employee was aware, or could reasonably be expected to have been aware, of the rule or standard … the rule or standard has been consistently applied by the employer. It is not possible to demonstrate “validity“ or “reasonableness“ if the relevant “rule or standard” is found in a guideline (which is optional) rather than an issue specific policy (which is mandatory). More importantly, however, is the fact that an employee might be able to raise the defence in a disciplinary enquiry that there was in fact no “rule or standard” as (if it is contained in the guidelines) the rule is merely optional and does not have to be followed.

IT Risk Management (Risk IT)

The Risk IT framework complements COBIT, which provides a comprehensive framework for the control and governance of business-driven information-technology-based (IT-based) solutions and services. While COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the ends by providing a framework for enterprises to identify, govern and manage IT risk.

The Risk IT framework is to be used to help implement IT governance, and enterprises that have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT.

The connection to business is founded in the principles on which the framework is built:

- Always connect to business objectives
- Align the management of IT-related business risk with overall ERM
- Balance the costs and benefits of managing IT risk
- Promote fair and open communication of IT risk
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and
- well-defined tolerance levels
- Are a continuous process and part of daily activities

3.1.2 IT Security (NIST)

The risks that come with cybersecurity can be overwhelming to many organizations. Building out a robust cybersecurity program is often complex and difficult to strategize for any organization, regardless of size. Frameworks are not a new concept to cybersecurity professionals. The benefits are immense – nor do they need to be complex to be effective.

This Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts:

1. Framework Core
2. Implementation Tiers
3. Framework Profiles.

The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles.

Through use of Profiles, the Framework will help the Township align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for the Township to view and understand the characteristics of their approach to managing cybersecurity risk.

The NIST framework (or one similar) would be implemented and managed by a third-party security provider as part of an overarching security service.

This is a great example of where a shared service led by the Counties could provide all lower-tier municipalities with enterprise cybersecurity management with a substantial cost savings.

3.1.3 IT Service Management (ITIL)

IT Service Management (ITSM) is a common term used for describing a strategic approach ideal for designing, delivering, managing, and also enhancing the manner in which information technology (IT) is employed in an organization. The ITIL ITSM framework is responsible for guaranteeing that the correct processes, technology, and people are in place, thus enabling the organization to meet its business- related goals.

The way to choose the right ITSM processes for the Township, is to look at what the business specifically needs. For instance, for organizations the size of the Township that are typically managing the same issues, it makes more sense to find the root cause and resolve it once and for all. A simple example of it would be a storage space issue on the FileHold server at the Township – you can keep deleting files and applications every time the hard drive hits its capacity. But simply installing a bigger hard drive is a better longer-term solution.

In ITSM terms, it translates to going from mere Incident Management to Problem Management. In the example above, the FileHold server running out of storage space is the incident and the hard drive capacity being inadequate is the underlying problem. Of course, IT support teams in larger organizations typically handle incidents that are much more complex and send problems over to dedicated problem management teams.

That being said, the primary component we are addressing in this report pertains to It Service Continuity (a subset of Business Continuity)

IT Service Continuity Management (ITSCM)

By definition: IT Service Continuity is a subset of Business Continuity Planning (BCP) and encompasses **IT Disaster Recovery Planning** and wider IT resilience planning. It also incorporates those elements of IT infrastructure and services which relate to communications such as (voice) telephony and data communications.

The IT Service Continuity strategy is the “technical component” that’s aligned to the Business Continuity Lifecycle and helps you to prepare for the worst case scenario; that is not just how to recover from a disaster but to stop the disaster from occurring in the first place, if at all possible.

Using disciplines such as ITIL’s IT Service Continuity Management (ITSCM), these activities investigate, develop and implement recovery options when an interruption to service reaches a pre-defined point. It must be a part of the overall Business Continuity Plan and not dealt with in isolation.

By having such a plan, the Township can prevent an ad-hoc approach or individual appraisal in case an emergency situation takes place and continuity of IT services needs to be ensured. Both ITIL and ISO 20000 require companies to consider their business operations while establishing an IT Service Continuity Plan.

An ITSC strategy should define the direction and high-level methods that should meet IT service-level objectives. In formulating ITSC plans, organizations are advised to aim for a simple, clear, unambiguous and all-encompassing set of documents that define the actions required to restore IT services in the event of an incident.
The work recommended in this ITMP will help the Township determine, for YOUR installation, the “What is a Disaster?” description. Defining the pre-conditions that constitute a disaster is part of the process. Such definitions form an integral part of any Service Level Agreement (SLA) relating to the provision of services.

The strategy addresses risks identified with a potential to cause a sudden and serious impact, and items that could immediately threaten the continuity of the business. These typically include things such as:

- loss, damage or denial of access to key infrastructure
- application services failures

- non-performance (including the possibility of your provider experiencing disaster) of critical providers, distributors or other third parties
- corruption of key information
- sabotage, extortion or commercial espionage
- deliberate infiltration
- attacks on critical information systems

The ITSC strategy should be the collection of policies, standards, procedures and tools through which the Township not only improves its ability to respond when major system failures occur, but also improve their resilience to major incidents, ensuring that critical systems and services do not fail or that failures are recovered within acceptable process Recovery Time Objective (RTO) limits.

Business Impact Analysis (BIA) information is used to define the process RTO and determine the recovery prioritization. This makes the recovery process a user-centric activity matching business requirements.

The recovery plans are organized in a hierarchy:

1. A site loss plan details the systems which would be affected by the loss of a building.
    a. A separate plan for each service should provide detailed procedures and step-by-step guidelines for each stage of an incident so that the Recovery Teams are able to restore the services and thereby to meet the agreed process and component RTOs.

The plans should be clear and concise and expect a level of knowledge but not presume explicit local knowledge, in the event that external assistance is required to rebuild systems (the same is true of Disaster Recovery Plans). Each procedure should be self-contained so that it can be utilized to effect recovery of a single system or component (e.g. the server is running successfully but the database management system has crashed). Each document must also contain details of pre-requisites; this means that in the event of multiple component failures the correct sequence can be followed (e.g. replace failed disk, rebuild operating system, install database, configure security settings and then restore data).
IT Service Continuity Management (ITSCM) focuses on those events that the business considers significant enough to be treated as a “disaster”. Less significant events will be dealt with as part of the incident management process.

3.2 Use Technology & Strong Partnerships to drive Modernization of Business Practices

The previous section focused upon how the Township approaches and manages technology – these shifts in approach are crucial to future success and will have long lasting impacts.

This section focuses upon the technologies that the Township can implement and the partnerships it can leverage, under its new approach, to modernize and optimize business processes and practices.

The technologies recommended here have been implemented by other municipalities. They are not 'nice to have' features – they are 'must haves' which have proven their ability to help organizations deal with significant growth, to increase the productivity of staff, and to deliver services in the way that residents moving into the Township, or joining as staff, increasingly expect – via web browser and smartphone.

3.2.1 Implement New Infrastructure Systems (where there are none today)

Implement a VPN for access to SCADA Monitoring System (enhancement)
This system is running well but the method used to access it is a security risk to the Township. After discussions with the vendor (Capital Controls) it was agreed that a secure VPN (Virtual Private Network) would be the recommended approach in securing access to the systems supported within the Township.

Network Assessment
The Township should engage a third-party firm to provide a network assessment that will review the existing structure, and comprehensively assess the Township for cloud readiness. This will help to determine what potential solutions best yield greater efficiency, and smoother functioning, of the infrastructure.

This assessment could also extend to the Counties in order to explore alternatives to the existing MPLS link the Township currently utilizes to access the Vadim systems hosted at the Counties. The current network speed of 1Mbps/10Mbps is quite slow by todays standards.

This is a great example of where a shared service led by the Counties could provide all lower-tier municipalities with a third-party assessment at a substantial cost savings.

Mobile Device Management
The Township does not currently manage mobile devices. This is a critical function when we consider percentage of Township employees that carry corporate smartphones.

The Township should create a formal device policy that educates staff on security risks and best practices. But a general consensus isn't enough to protect Township data as it travels between numerous devices. For that, the Township will need a mobile device management (MDM) solution.

MDM software will provide central control of devices in the network, including device data, security, applications, web activity, and data transmission (depending on how the system is configured).

This is a great example of where a shared service led by the Counties could provide all lower-tier municipalities with a third-party MDM service at a substantial cost savings.

Cloud Storage Strategy
There are many opportunities to cost-effectively move inactive or stale data (as an example) to low cost cloud services. The Township should develop a strategy that would lower the cost/need to manage data in-house.

This process could start with a small data archiving pilot using one of the many cloud-based services available on the market.

3.2.2 Replace Existing Infrastructure Systems (as needed)

As illustrated in the MTA, the Infrastructure layer is the foundation for the entire technology environment. Infrastructure must be robust and reliable because it provides the foundations for all other layers. Unreliable infrastructure undermines all the technology that sits above it.

Email Services (Ignite Solutions)
The current email service is not considered "enterprise-class" and needs to be replaced immediately. The service offers what's called a basic "POP3/IMAP" service. There are no calendar or contacts synchronization features, although these are important requirements for the Township. Staff currently use secondary solutions such as Google Calendar as "isolated" solutions with no integration with the email system.

In addition to the functionality issues, the system is not redundant, putting the Township at risk of email outage and data loss.

3.2.3 Implement New Business Systems (where there are none today)

Effective municipalities rely on a combination of **people**, **processes** and **technology,** working together in a synchronized fashion, to deliver services to customers.

To deliver efficient and effective government services, those processes should be digitized – this represents a move away from paper-based or spreadsheet-based processes to electronic, online, workflow managed, real-time processes.

Digitization should be built upon a small number of powerful business systems such as:

1. **HR Information System (HRIS)** – Implementing a proper HRIS solution will eliminate inefficiencies that exist today, providing the Township with digital capabilities for HR Management (employee records, benefit tracking), Employee Self-Service, Hiring and Onboarding, etc.
2. **Payroll** – Ideally integrated with an HRIS system, this system will simplify Township management of taxes, deductions, and accruals tracking. Employee self-service capabilities would further facilitate productivity and efficiency.
3. **Asset Management** – The Township is currently applying for a grant from the Canadian Federation of Municipalities "Municipal Asset Program" that would help advance the procurement of an Asset Management solution. Upon acceptance of this grant, the Township would have 11 months to purchase the solution.
4. **Fire Management System –** The process of moving to a digital platform was initialized during the engagement. The Township is negotiating with BeeOn solutions, an organization that specializes in Fire MS.
5. **Work Order Management** – It is recommended that the Township implement the Asset Management solution first, and then develop proper processes to support the implementation of Work Order Management.

These systems will help drive much of the operation of the Township and today they represent major gaps in technology.

The business systems used should be common and shared across departments and divisions so that tasks initiated in one area can be allocated to another; so, for example, a change in a permit application status (in Building) could trigger the processing of a pre-approved payment (in Finance).

The full digitization of processes provides the foundation for becoming an efficient organization.

When processes are digitized and managed electronically, all necessary transaction processing - workflows, notifications, quality checks and validations - can be carried out via a device, and can happen anywhere (in the office, at a worksite, in a truck at the side of the road, or at home).

Offline steps (manual interventions such as checking a paper file or getting a physical signature) are reduced or eliminated. The online chain provides complete visibility of the process throughout the organization – anyone can check the status or find out required information. Systems manage the routing and workflow of the processes, including escalating items to senior staff when exceptions are encountered, or where performance falls below defined levels of service.

Digitization allows the Township to track its own processes, to share information between staff, and to track important management metrics that provide insights that contribute to improved process effectiveness.

As noted in the MTA assessment in Section 2 there are a series of business systems that are currently missing. So, a significant portion of the work envisioned by the Strategy focuses upon addressing these gaps and digitizing important work processes such as payroll, asset and work order management among others.

3.2.4 Replace Existing Business Systems (as needed)

Although having no systems to replace manual processes would be a major challenge for most organizations, systems that lack functionality or pose a risk to the corporation can be equally painful.

There are several systems that fall into this category:

eAgenda Sofware (Council Docs)
The current solution (Council Docs) has outgrown its usefulness at the Township. Developed by an ex-employee at the Counties, this solution does not provide the functionality or support required at the Township. The lack of features and overall state of the product, although at one point may have served a purpose, is long overdue to be replaced by a COTS (commercial off the shelf) alternative.

Building Permit (Proware)
Although this solution seems to satisfy most of the Township requirements, there's a risk to the organization when we consider that the solution is supported by a single developer (Proware). This vendor has two employees -one of which is the developer. In addition to the vendor risk, the product lacks some functionality with further development in question. As part of the new initiative to implement sound Technology Management Frameworks as outlined in the previous section, we are recommending that an alternate solution be researched and sourced.

In parallel to this, we are recommending that the Township test the exporting of Proware data to a "CSV" (flat file) to ensure a smooth migration process when a new system is procured.

3.2.5 Enhance/Upgrade Existing Systems (as required)

There are systems that are currently in need of enhancements or upgrades. Some of the recommendations in this section will also pertain to integration and training - it seems that in some instances the system functionality exists, but the Township lacks the formal training to leverage said functionality.

Vadim (system review)

The current climate of frustration with respect to Vadim functionality, performance, and support has continued to escalate within the Township. A formal analysis is recommended that details these issues, allowing the Township to determine the appropriate strategic direction for this system.

FileHold (training)

This solution was purchased in 2016 and is a leader in records management within the municipal space. There have been issues with the staff at the Township using the product, with complaints in our discovery phase ranging from "difficult to use" to 'hard to find documents".

Our assessment is that a formal scheduled training program must be developed with the vendor (ImageAdvanatge). The vendor has agreed to provide "no cost" onsite training quarterly, with remote training also available at no cost at any time.

BookKing/Vadim (Integration)

The Recreation department currently relies on manual deposits since there is currently no integration with Vadim. This is an inefficient process. Program registration is combination in-person & online process tracked in a spreadsheet and manually moved over to Finance for input into Vadim. The vendor (BookKing) can offer online payments, but can't do this now due to lack of Vadim integration.

It was discovered during out assessment that a BookKing module exists within Vadim, but this was never communicated. We are recommending that this be explored immediately.

3.2.6 Adopt Cloud Services and Solutions

Given previous discussions about pressures on internal infrastructure resources – one approach to reducing the infrastructure pressures is through the adoption of cloud services. This is an industry paradigm that has gained steam in recent years, to the point where it is becoming increasingly difficult in some areas (e.g. HR systems) to find vendors that provide on-premise solutions. Many municipalities have moved to the cloud for email services (Office365, G-Suite), or are in the planning stages.

The Township should pursue cloud solutions as a strategic direction and thus will need to establish a clear policy statement and framework for assessing that cloud solutions meet the Township's security and privacy, resiliency and continuity requirements (as recommended in this report).

3.2.7 Increase Digital Delivery of Township Services

Customers increasing deal with their institutions – their bank, insurance firms, Service Ontario, or the CRA – online or via apps on smartphones. Netflix has over-taken cable TV, websites have overtaken newspapers and magazines. Increasingly customer expectations are that they can interact with the Township electronically – in ways that are less disruptive and more convenient than current ways.

Others have characterized the way municipalities provide services as "Blockbuster service for Netflix customers" – an outdated service delivery model that no longer meets the expectations of customers.

Beyond customer expectations, there are clear financial imperatives for the Township to offer and encourage the use of services online. Studies into channel costs suggest that a face to face customer interaction costs up to $30 per transaction, a phone transaction costs between $5 - $7, and a web transaction between $0.15 – $0.90. Quite simply, it is cheaper for the Township to transact online than face to face or via the phone.

So, while this digital services may be the long term target for the Township, there are pre-requisites that must be in place before the Township can offer such services. Processes must be digitized first before services can be offered online.

3.3 Summary

In summary the strategy focuses upon the following areas:

- Elevating the importance of technology management frameworks within the Township
- Using these frameworks to develop sound Disaster Recovery Planning (DRP), policy development, cybersecurity management, and risk management
- Using technology and strong partnerships to drive modernization of business practices
- Implement systems for key services that are manual today, and update/replace others as required
- Embrace the cloud and increase the digital delivery of Township services

Please refer to Appendix C for a high-level diagram that illustrates a potential future infrastructure (Phase 1)

4. Major Initiatives

The following section outlines the major projects that are recommended.
Please note: for projects that could be opportunities for a Counties led “shared service” approach we have denoted with ***Shared Service Opportunity**

4.1 Major Infrastructure Projects

As identified in the findings a series of technology infrastructure projects are required to establish robust, reliable foundations for the future.

4.1.1 Implement Office 365

It is recommended that the Township evaluate the move to Office 365 – Microsoft’s cloud-based office system. Initially, email services should be moved into the Microsoft cloud, providing a range of features, including flexible remote access from a variety of devices and larger mailboxes, whilst reducing management, storage and hardware overheads.

Office 365 capabilities including broader access to Office products (staff can install on various devices, including tablets and phones) will also be leveraged.

Additional features of Office 365 (including OneDrive, SharePoint, Skype for Business, Teams) and other collaboration capabilities will also be considered but require more detailed planning and consideration before being deployed.

4.1.2 Initiate IT Policy Development

Today the Township has no IT policies. As part of this engagement PGC will provide the Township with two or three sample policies in order to help initiate the process. The Township needs to focus on a few key policies as starting points (e.g. acceptable use, passwords, security, backup, cloud, etc.).

Once these policies have been formally adopted the Township can continue developing corporate IT policies as required.

4.1.3 Disaster Recovery (ITSCM) Readiness

As a major part of IT Governance, the Township must be more prepared for business continuity in the event of an incident impacting the Town’s data centre. Although it may seem unlikely, events do happen – for instance the County of Huron technology systems were heavily impacted when a tornado damaged the County building in which their data centre was housed.

We recommend that a formal IT Service Continuity plan should be developed, a technology disaster recovery response plan should be put in place that identifies the priority systems that must operate in the event of an emergency and the priority order in which systems should be recovered.

In the past municipalities built their own disaster recovery sites, but today municipalities are typically implementing Disaster Recovery as a Service (DRaaS) – with hosted service providers as the most cost-effective approach. It is recommended that the Township follow the DRaaS approach.

4.1.4 Mobile Device Management

Once the Township develops a policy for Mobile Device Management (MDM), the recommendations are for a third-party provider to deliver these services through the cloud. This has become somewhat of a commodity play and will present a good opportunity for the Township to have the management of all corporate devices out-tasked for a fairly low cost. **Please refer to Appendix E for an overview or MDM options.**

***Shared Service Opportunity**

4.1.5 Collaboration Capabilities

Encouraging and facilitating easy collaboration between staff, partners and the public is the goal. There are various tools and capabilities in the market that municipalities are taking advantage of. These include:

- Email
- Unified Communications
- Digital Meetings (voice, video, screensharing)
- Messaging / Chat
- Enterprise Social Networks
- Intranets
- Blogs and Wikis
- Collaborative File Editing / Co-Authoring
- Enterprise File Sync & Sharing (EFSS)
- Large File Transfer
- Team / Project / Partner Collaboration
- Workflow management
- Document / Content Management

Following on from the Office 365 assessment, when the Township has a good understanding of the capabilities of Office365 the Township should determine its overarching approach to Collaboration technologies. SharePoint and Office 365 may address some needs, but may not meet others. The Township should determine which areas of collaboration are important (for example, unified communications, digital meetings, collaboration spaces and Wikis) and then should determine which tools are suitable for the Township to adopt and implement.

It should be noted the existing records management solution FileHold has a SharePoint module that would allow for integration.

4.1.6 Managed Security Service

As part of this engagement, the Township has invested in a high-level security assessment that result in numerous gaps that need to be addressed. The Township has obligations to keep its information secure. Reading the news in 2018, shows how important security has become – for instance the Town of Wasaga Beach was recently hit by a ransomware attack.

Smaller municipalities are even more challenged to keep up with security threats due to limited resources and the requirement for senior security services. It is recommended that an external security firm be retained to conduct ongoing security operating activities – monitoring, alerts, security assessments, and to provide advisory services.

In addition, annual security re-assessments are planned to confirm current situation and identify improvements. It should be clear that information security is an ongoing concern, which will require ongoing funding and attention to maintain a secure environment.

***Shared Service Opportunity**

4.1.7 Implement VPN Solution (3 water/wastewater plants)

The security risk in the management of the SCADA system at the 3 water/wastewater facilities is fairly easy to address and should be carried out by the vendor who supports the system (Capital Controls). This would mitigate the risk of another third-party attempting to implement a solution on core systems they do not currently support.

4.1.8 Network Assessment/Managed Network

The Township needs to evaluate its network situation (all sites) and determine the best approach to delivering services both internally and through cloud service providers. This process could lead to a managed network opportunity if in fact the cost-benefit proved to be favourable.

Currently there is no connectivity from remote sites into the Township, but the cloud strategy and other activities will in fact determine if this is required.

***Shared Service Opportunity**

4.1.9 Ongoing Maintenance Activities

It is important to note that these major technology initiatives are in addition to a range of ongoing infrastructure maintenance activities, which includes network and switching hardware renewal, end user device replacements, and storage technology replacement. Each of these initiatives will mitigate corporate risks, are critical to maintaining operations and must be planned and resourced as part of the annual work plan.

4.2 Major Business Solutions

The Township has several major gaps in its business systems platforms that will be critically important to address over the coming years.

4.2.1 Payroll and HRIS Strategy

The Township is currently using manual processes for payroll and there is no HRIS system in place. It is recommended that a clear HRIS strategy and roadmap be developed and discussions with similar sized municipalities who have recently procured these systems be leveraged for insight. As an example, the Town of Georgina recently implemented an HRIS SaaS solution from Bamboo and they're quite pleased. The costs for these services are fairly low and most have partners that integrate Payroll capabilities into their solutions. The vendor (Bamboo) will have a Payroll module integrated Q1 2019.

4.2.2 Asset and Work Management Systems

The Township, like many municipalities is investing in Asset Management, and strategies to effectively and sustainably manage the lifecycle of its assets. There are two core systems associated with Asset and Work Management which the Township should invest in (separately):

- **Asset Management Systems**. These solutions typically include valuation, planning and decision support tools, and they help the Township more effectively plan asset management activities to predict future funding needs, to model scenarios and to achieve and/or prolong the lifecycle of assets. Currently the Township has applied for funding from the Federation of Canadian Municipalities Municipal Asset Management Program. Upon program approval the Township will have 11 months to secure a solution. In addition, the Counties has selected Public Sector Digest (PSD) as their AM solution. The Township has researched multiple solutions to date, and has a preference for the PSD solution. The cost would be $40,000.00 (year 1) and $7,000.00 annually from year 2 onward, This pricing does not reflect any grant funding from the FCM program.
- **Work Management System**. These systems are needed to effectively track assets and the work that is done against the assets (inspections, planned maintenance and reactive work). These systems typically involve asset registers, service requests, work order management, GIS integration, mobile systems access for field crews and online service request deployment. They help improve the productivity of crews and provide management information about resource allocation and utilization. Typically, these systems may be used for linear (road, water, waste and storm water), facility and fleet assets.

It is recommended that the Township first confirm the requirements and solution for Asset Management (and the integrations) that will be needed to meet those requirements. There are significant systems, data and process integration issues that need to be tackled to address this initiative effectively. This is a large program of work that could be a multi-year endeavor to implement the initial solution, and to become fully adopted across the Township.

With respect to Work Order (Management) the Township needs to first adopt inter processes that will support the system. This system should following the Asset Management system (2020).

As part of large projects such as these, it is important to focus upon business process design. As an illustration, the City of Cambridge (a municipal leader in work and asset management) rationalized their work management processes into 12 common process (Service Request, Work Order, Inspection, etc.) before implementing their Work Management solution. This achieved significant productivity benefits and reduced overall implementation costs; a strategy that the Township could follow.

Also note that implementation of these types of systems requires operational resources to train and support, sustain and evolve the solution. Kitchener, for example, has three staff members in the Operations Division dedicated to supporting their Cityworks implementation, alongside two staff in IT.

4.2.3 By-law Enforcement System

The Township currently leverages AccessE11 to track every law enforcement case. However, users are frustrated with the limitations of the product since this system was developed with public works in mind. There needs to be further investigation into the possibility of enhancing the current solution to meet the needs vs. alternative solutions.

4.2.4 Fire Management System

There is currently no management system in place for Fire. They require a system that provides more information for liability for the Township. e.g. insurance companies are now asking for information that Fire do not have in using the OFM website. They have a manual process that is inefficient and presenting a risk to the Township.

Other local municipalities are using a hosted product called BeeOn. This vendor is based in Quebec and seems to be a suitable partner for the Township. All modules are entirely integrated and perform complete management of human resources, inventories, prevention components and emergency-responses. The software also features web and mobile applications offering unmatched field flexibility.

4.3 Integration

4.3.1 Integration Technology

The Township needs to increase its capability around systems integration, and to simplify integration implementation and maintenance – to improve data integrity and to reduce manual work. It must become easier to implement and maintain integrations and interfaces. Increasingly those interfaces will need to operate across on-premise and cloud-based environments and be web-service based. It is recommended that the Township implement integration technologies to simplify integration development and support. An example discussed in this report is the requirement to have Vadim integration with BookKing. Future examples may be HRIS and Payroll or SharePoint and FileHold.

4.3.2 Data Standards

Given the importance of data to the organization, and the potential around analytics, the Township must focus attention on data standards and its data architecture. Defining data standards around Assets, People (customers and employees) and Location (address, streets) are the areas that will have the highest impact and will be supportive of planned initiatives such as Work and Asset Management projects.

4.4 Customer Facing Solutions

4.4.1 Online Services

Although the Township are migrating to a new dashboard for their website, there are many opportunities to enhance the services that are currently being delivered. The current situation with the Counties has resulted in miscommunication and a general waste of staff time trying to move forward with developing a proper site that includes eServices such as:

- Online maps
- Where to eat within the Township
- Snow plow routes
- Marriage certificates
- Building permits
- Planning applications
- Dog licenses etc.

Municipalities of similar size have implemented all of the above, and more. The Township can leverage municipal vendors such as eSolutions who can provide discounts when multiple municipalities share ongoing support. The cost savings can easily be 30% or more.

***Shared Service Opportunity**

5. Implementation Plan and Budget Implications

5.1 Major Initiatives – 2018 Task List

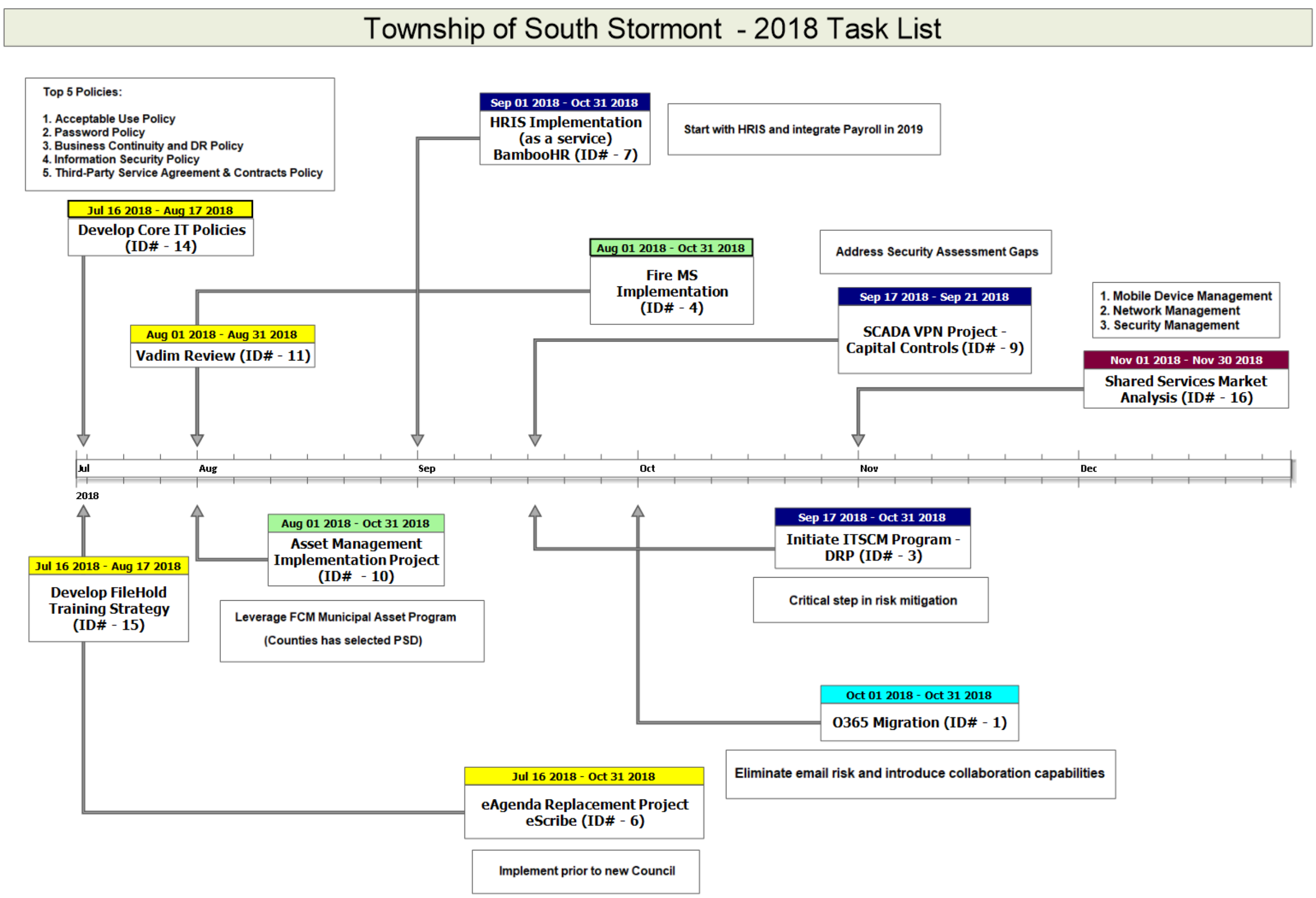
The following timeline identifies the recommended strategic initiatives to be considered as "Phase 1" activities as part of the funding allocated for IT. Few initiatives are earmarked for the last year, to accommodate slippage and to acknowledge that some projects will get delayed due to unforeseen circumstances (e.g. delays in software releases, etc.).

The projects listed in Figure 5 are to be consider the core activities anticipated to initiate in 2018. Some of which may flow into 2019 depending on delays.

Please refer to Appendix E for a detailed 3-year Work Plan (2018 – 2020)

Please refer to Appendix G for an expanded image of Figure 5

Figure 5: *Township of South Stormont Key Initial Projects (2018)* ***NOTE:*** *ID#'s in the task list correspond with the compete task list in the Work Plan (Appendix E)*



5.2 Additional Considerations

5.2.1 Servers

With the continued move to a more "cloud-based" model of operations, the Township does not need to allocate any additional funds to server hardware at this time. The one item that was raised was the single domain controller (no redundancy). This can be resolved by having the Counties configure a secondary server at their location to be used as a backup over the MPLS network.

By 2020, the landscape at the Township may be changed to the point that the FileHold server may in fact reside in the cloud. In the meantime, the existing (leased) FileHold server could be purchased outright for under $1,000.00.

5.2.2 Desktops

Staff are using devices (iPad's, smartphones and Chromebooks) and services (Facebook, WhatsApp, Uber) in their personal lives that are simple and easy to use. They are looking for the same, flexible, consumer friendly technology at work that helps them get stuff done, not a hindrance. Thus, adopting consumer technologies, moving from desktops to laptops, **for staff that require mobility**, and providing tablet options is one area that modernizing services should be a focus.

It is recommended that the Township identify employees requiring mobility and consider laptops or tablets with these staff members. Some staff may also be sharing a desktop, in which case a traditional approach may make the most sense.

As the Township moves forward with more cloud initiatives, many users will only require a browser to access corporate applications (especially true if Office is in the cloud). Lower cost small form factor PC's (e.g. Dell OptiPlex) can allow for local installations of Office and decent power with a small footprint and price point (under $800). For senior management and Council, laptops can be purchased outright for approximately $1,200.00.

Industry trends are seeing PC refresh cycles slowing down to 5 or more years. When we consider the cost to lease a PC or laptop ($50 - $100 per month), a new unit can be purchased outright and paid off in less than 2 years.

The Township requires 12 laptops and 4 desktops in 2018. Moving forward into 2019, it is recommended that a short study be carried out to analyze the state of the remaining PC's and determine the best strategy for future replacements.

5.2.3 Shared Services Market Analysis

In considering the potential for a "Shared Services" model with the Counties and lower-tiers, the Township should consider going to market (RFI or RFQ) to obtain comparison pricing for the following services being considered:

1. Network Management (as a service)
2. Security Management (as a service)
3. Mobile Device Management (as a service)

5.2.4 Digital Signature Solution

Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature (eSignature). The Township needs to investigate the various options in the market and select a solution (e.g. Adobe, DocuSign)

5.3 Budget Summary Estimate (by year)

2018		2019		2020	
One Time	Recurring	One Time	Recurring	One Time	Recurring
$67,000	$17,800*	$48,500	$55,000	$20,000	$60,000
*$1,483 per month amortized over 1 full year					

Notes:

- The majority of solutions are "cloud-based" and therefore recurring operating expenditures.
- Year 1 (2018) includes the purchase of 12 laptops and 4 desktops
- Year 2 (2019) & Year 3 (2020) include a recurring cost of $20,000.00 for managed security. A shared service would lower this to approximately $6,000 per year.
- Recurring costs for Year 1 (2018) are based on a full year of service. The estimate is $1,483.00 per month amortized over 12 months.
- "one-time" costs for 2020 projects have been estimated at $20,000. The primary implementation listed in the work plan are By-Law and Work Order systems. There is insufficient information at this time to estimate the Work Order system due to a lack of Township processes to support this initiative.

Appendix A – Security, Operations, & Data Management Scorecards

Township of South Stormont – Security Assessment (Part 1) Policies – Governance – Risk Management – Vulnerability Assessment – Intrusion Testing		
Area (+ total rating)		**Assessment**
Policies Asset Classification – Policies		Currently, no formal asset classification scheme is in place. Nothing formally outlines these definitions and dictates handling of various categories of assets. Policy documents are lacking and are also not centralized.
Governance Frameworks		At this time, no governance framework is in place.
Risk Management Processes		The IT group being generally comprised of mature and experienced workers naturally gravitates to what appears to be a reasonably secure state (however nothing formally validates this). IT decisions in the past appear to have been ad-hoc (no risks analysis).
Vulnerability Assessment Continuous Monitoring		No continuous vulnerability testing is in place using industry-recognized tools. A past vulnerability audit was performed in 2014, however many of the recommendations in this past audit have not been addressed.
Intrusion Testing Test Cycles and depth		Annual intrusion tests are not being performed. During this audit, some light tests were performed that uncovered some significant weaknesses, however the tests performed are not complete – they do not cover the surface area to which the infrastructure is exposed.

Recommendations

- **Policies** - The creation of an asset classification policy is the next step to increment the maturity in this area. Once a classification and labeling scheme is agreed to, the current policy documents need to be reviewed and adapted to the new classification schema. This step should include reviewing the existing policies and adapting them to a more complete set of policies that will cover the key areas common in IT dependent enterprises.
- **Governance** - As enterprise IT grows, an appropriate governance framework could be considered. At this stage, the size of the Township (and associated IT team) does not work well with most frameworks due to the overhead and associated tasks that come with performing governance activities. This implies that a simplified framework (custom) should be considered.
- **Risk Management –** Next Steps: **1.** Implement a security opinion process where technological changes or concerns are brought to a qualified security expert for comment and direction **2.** Identify a risk management process (starting off with a light process and adding to it as time goes by and the need dictates further analysis) **3.** Integrate risk management process with current business processes such as project management, change management, help desk, etc. **4.** Monitor for thoroughness (does everything go through the risk management process) **5.** Determine the Townships comfort level based on contractual obligations and identify the type of cyber insurance that can be obtained to reduce the Townships financial exposure
- **Vulnerability Assessment -** Next Steps: **1.** Deploy or retain a vulnerability testing solution that performs testing monthly (minimum) **2.** Ensure solution provides trending statistics and provides actionable reports (various views on vulnerable data) **3.** Ensure a technical resource is assigned to review the findings **4.** Ensure KPI's are presented to management **5.** Integrate application
- **Intrusion Testing -** SOUTH STORMONT needs to improve its security processes such as automatic updates, hardening of servers and workstations, and review of network hardware hardening processes. We are aware that such processes are particularly difficult because of the intrinsic nature of the SOUTH STORMONT infrastructure. However, for the same reason, the infrastructure is potentially subject to attacks by motivated attackers.

Township of South Stormont – Security Assessment (Part 2) Alerting & Response – Physical Security – Security Awareness – Configuration Assessment – Third-Party Security		
Area (+ total rating)		**Assessment**
Alerting & Response Visibility – Tools		No ITIL type process is being followed. The staff currently handling cyber incidents has no formal security training or certifications. Only major failures are documented and statistics kept. No formal incident management process is documented.
Physical Security Measured Controls		No formal physical security reviews have been performed. No documentation exists, and no past physical audits have been performed and could be reviewed.
Security Awareness Processes		No program for security awareness is in place
Configuration Assessment Health of IT Assets		No hardened configuration has been designed or tested on. The hardware/software deployments are standardized but baselines are not compared.
Third-Party Security Security Evaluation		No evaluations of 3rd Parties has been done from a security point of view. Contracts do not include clauses that allow security testing, and if a supplier claims to have been audited, you do not check these audit results and ensure they have taken action on mitigation.

Recommendations

- **Alerting & Response** – Next Steps: **1**. Document a formal incident response process **2.** Ensure that appropriate responsibilities are assigned and that a cyber expert is included in the workflow (this can be a third party that you could call on in the event you need additional assistance). **3.** Document events of all levels to assist in future event resolution (post-mortem is crucial) **4.** Ensure you have the ability to reach all pertinent individuals should an emergency take place **5**. Identify solutions for detecting advanced persistent threats (lateral movement, intrusion detection, data leakage, file integrity alerting, etc.) and provide this data to a centralized event correlation system **6.** Provide cyber training to key individuals and when staff shows adequate aptitudes get them formally certified.
- **Physical Security -** Mandate a physical security audit of key Township locations and prioritize findings. Resolve any significant issues identified during this audit and ensure physical security is addressed for any new projects.
- **Security Awareness –** Identify a security awareness-training partner (or other solution) and review their awareness training material. Identify any areas that require changes to adapt to current Township culture. Roll out the program with the assistance of HR and ensure that a documented trace of each staff taking the training is maintained throughout the year.
- **Configuration Assessment -** Identify hardened system baselines (hardening standard to be used). Customize selected standard to meet Township requirements and ensure systems are configured following the newly identified baseline. Configure a configuration management testing solution to validate compliance.
- **Third-Party Security -** Identify the initial 3rd party security questionnaire that is submitted to all third parties yearly and document all responses. Follow up with questions based on their initial answers and document any risks identified, feeding them into the risk management process if pertinent. Ensure that your contracts allow you to "test" the vendor's security on a case-by-case basis. Ensure that you review any claimed audits and the vendors resolution plans and progress.

TOWNSHIP OF SOUTH STORMONT – OPERATIONS ASSESSMENT IT GOVERNANCE – BUSINESS CONTINUITY MANAGEMENT – IT SERVICE MANAGEMENT		
AREA (+ TOTAL RATING)		**ASSESSMENT**
IT GOVERNANCE Frameworks - Toolkits		The Township is not following a formal IT Governance framework (e.g. COBIT)
BUSINESS CONTINUITY MANAGEMENT ITSCM – Disaster Recovery		There are no Business Continuity or Disaster Recovery plans in place
IT SERVICE MANAGEMENT Policies and Processes		Although a basic "helpdesk" solution tracks issues, there are no formal frameworks being followed for ITSM (e.g. ITIL)

RECOMMENDATIONS

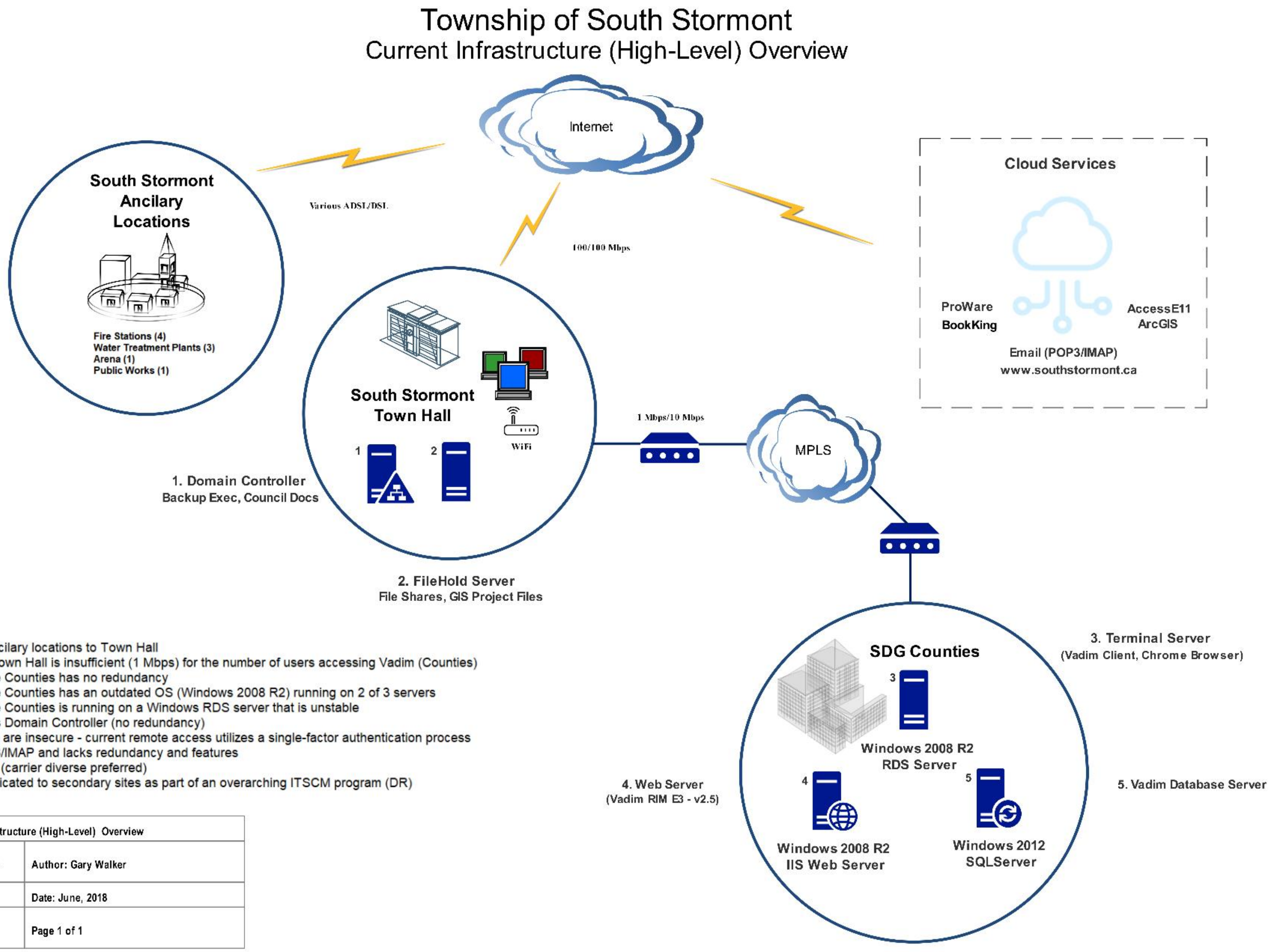
- **IT Governance** – Select an industry leading framework such as COBIT and start by addressing three critical areas: 1. Initiate an IT Steering Committee to help with technology decision making. This can include trusted partners. 2. Start formalizing key IT policies pertaining to acceptable use, password requirements, data backup, cloud computing, security, etc. Finally, develop a formal Risk Management framed such as RISK IT from the creators of COBIT. These should all be ongoing programs. We recommend an approach for the Township which clearly differentiates between issue specific, operational policies, standards and procedures, each of which should be set forth in separate documents.
- **Business Continuity Management -** Mandate the initiation of a formal IT Service Continuity Management strategy. This will include subset strategies around Disaster Recovery and Incident Response. Start with a Business Impact Analysis and IT Risk Assessment (closely aligned with ITSM). The IT Service Continuity strategy is the "technical component" that's aligned to the Business Continuity Lifecycle and helps you to prepare for the worst case scenario; that is not just how to recover from a disaster but to stop the disaster from occurring in the first place, if at all possible. Using disciplines such as ITIL's IT Service Continuity Management (ITSCM), these activities investigate, develop and implement recovery options when an interruption to service reaches a pre-defined point. It must be a part of the overall Business Continuity Plan and not dealt with in isolation.
- **IT Service Management –** Develop a formal framework such as ITIL. The ITIL ITSM framework is responsible for guaranteeing that the correct processes, technology, and people are in place, thus enabling the organization to meet its business- related goals. However, the Township may incur significant risks if it automates everything without maintaining the requisite knowledge of how to do things manually when something breaks. Therefore, following IT Service Management best practices is recommended.

TOWNSHIP OF SOUTH STORMONT –DATA MANAGEMENT SCORECARD DATA LIFECYCLE MANAGEMENT – DATA CLASSIFICATION – DOCUMENT MANAGEMENT		
AREA (+ TOTAL RATING)		**ASSESSMENT**
DATA LIFECYCLE MANAGEMENT Tiering – Archiving		The Township is not following a formal DLM process at this time
DATA CLASSIFICATION Categorizing – Organization		There are no Data Classification policies in place at this time
DOCUMENT MANAGEMENT Track – Manage - Store		The Township utilizes a Document Management System (FileHold) but there needs to be formal training to properly leverage the capabilities of the software. Users complain that the system is not intuitive

RECOMMENDATIONS

- **Data Lifecycle Management** – Create a complete data management policy – Having clear cut guidelines is the only way to get the Township on board and participating in a new data lifecycle management structure. Once you've defined the processes for handling data storage, backup, management, archiving, and deletion, you'll want to sum these up in a thorough data management policy. This policy should be shared with everyone in the Township so that they're made aware of the new process and can begin putting it into place. Perform an analysis of all unstructured data. Anything that's not been access in >1 year could be a candidate for offsite/low cost archiving.
- **Data Classification -** Start by creating a data classification policy. A data classification policy provides a way to ensure sensitive information is handled according to the risk it poses to the organization. All sensitive information should be labeled with a "risk level" that determines the methods and allowable resources for handling, the required encryption level, and storage and transmittal requirements.
- **Document Management –** Develop a training strategy and the rating for this area will easily improve.

Appendix B – Current State Infrastructure

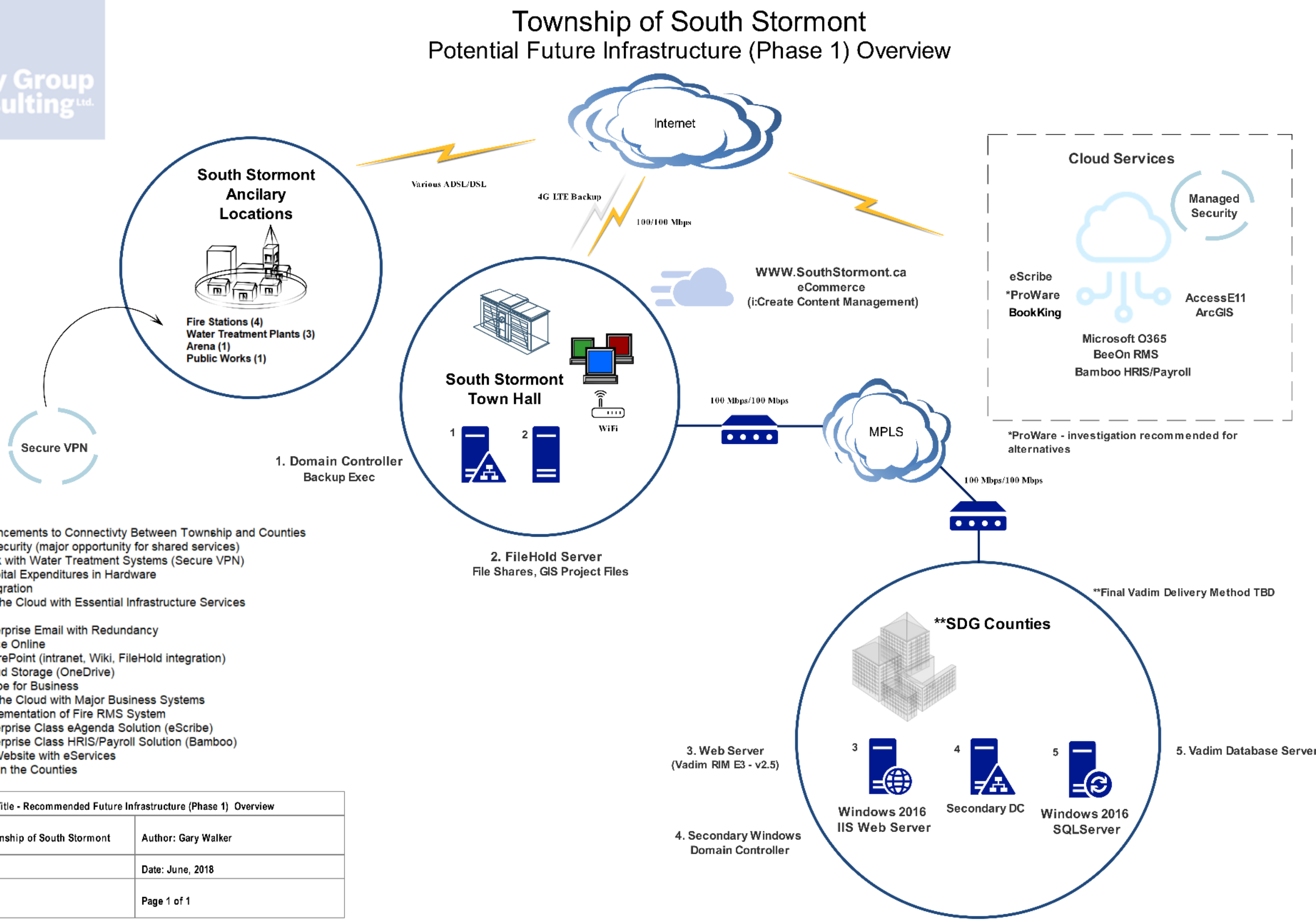


Current Challenges

- There is no connectivity from Ancilary locations to Town Hall
- The MPLS upload speed from Town Hall is insufficient (1 Mbps) for the number of users accessing Vadim (Counties)
- The Vadim system hosted by the Counties has no redundancy
- The Vadim system hosted by the Counties has an outdated OS (Windows 2008 R2) running on 2 of 3 servers
- The Vadim system hosted by the Counties is running on a Windows RDS server that is unstable
- Town Hall has a single Windows Domain Controller (no redundancy)
- The water treatment systems (3) are insecure - current remote access utilizes a single-factor authentication process
- The cloud email service is POP3/IMAP and lacks redundancy and features
- There is no Internet redundancy (carrier diverse preferred)
- There are no systems being replicated to secondary sites as part of an overarching ITSCM program (DR)

Title - Current Infrastructure (High-Level) Overview	
Customer: Township of South Stormont	Author: Gary Walker
Version ID: 1.0	Date: June, 2018
Comments:	Page 1 of 1

Appendix C – Potential Future Infrastructure (Phase 1)

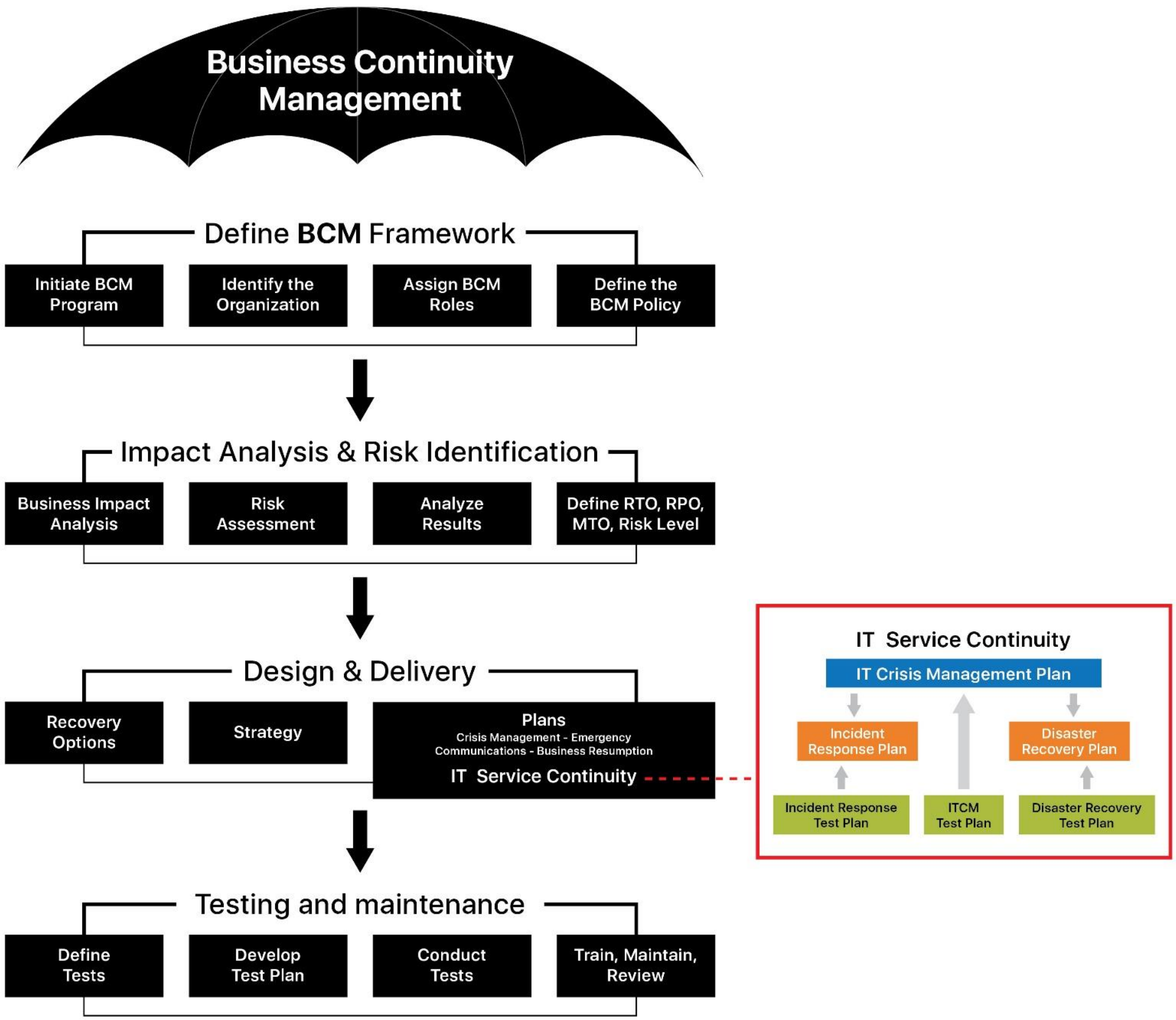


Benefits

- Major Enhancements to Connectivty Between Township and Counties
- Managed Security (major opportunity for shared services)
- Mitigate Risk with Water Treatment Systems (Secure VPN)
- Limiting Capital Expenditures in Hardware
- Vendor Integration
- Embracing the Cloud with Essential Infrastructure Services
  - O365:
    - Enterprise Email with Redundancy
    - Office Online
    - SharePoint (intranet, Wiki, FileHold integration)
    - Cloud Storage (OneDrive)
    - Skype for Business
- Embracing the Cloud with Major Business Systems
  - Implementation of Fire RMS System
  - Enterprise Class eAgenda Solution (eScribe)
  - Enterprise Class HRIS/Payroll Solution (Bamboo)
- Corporate Website with eServices
- Leader within the Counties

Title - Recommended Future Infrastructure (Phase 1) Overview	
Customer: Township of South Stormont	Author: Gary Walker
Version ID: 1.0	Date: June, 2018
Comments:	Page 1 of 1

Appendix D – IT Service Continuity Management



Appendix E – Workplan

Township of South Stormont Workplan								
Highlighted Projects Denote Shared Service Opportunity						**2018**	**2019**	**2020**
ID[9]	**Project Name**	**Comments**	**Who**	**Effort Days**	**Annual Budget**			
1	Microsoft Office 365 Migration (O365)	Year 1 (one time) cost of migration services	3rd party	30	$5,000.00	■		
2	O365 Annual Subscription (E1)	Pricing based on an estimate of 40 users @ $125/yr. per user. **NOTE:** Year 1 would be discounted based on service initiation	3rd party	N/A	$5,000.00	■	■	■
3	BCP/DR Readiness	Develop ITSCM Program (incl. BIA/RA)	3rd party	45	$8,500.00	■		
4	Fire MS Solution Implementation	Recommend: BeeOn Fire MS (one-time s/w cost)	3rd party	60	$9,000.00	■		
5	Fire MS Solution Maintenance	[10]BeeOn RMS - Annual Subscription Costs. **NOTE:** Year 1 would be discounted based on service initiation	3rd party	N/A	$2,300.00	■	■	■
6	eAgenda Replacement	Recommend: eScribe (SaaS) (w/ FileHold integration)	3rd party	60 - 90	$6,500.00	■	■	■
7	HRIS System Implementation	Recommend: Bamboo (SaaS). **NOTE:** Integrates with Vadim	3rd party	30	$5,000.00	■	■	
8	HRIS SaaS	Bamboo Annual Hosting Costs based on 40 users @ $8/user. **NOTE:** Year 1 would be discounted based on service initiation	3rd party	N/A	$4,000.00	■	■	■
9	SCADA VPN	Capital Controls: Current access process not secure. Require 2-factor authentication via VPN	3rd party	5	$5,000.00 - $10,000.00	■		
10	Asset Management	Consider leveraging Counties purchase of PSD - Township has applied for 2018 FCM grant	3rd party	60 - 90		■	■	■
11	Vadim Review	Analysis and roadmap	TBD	10	$5,000.00	■		
12	PC Upgrades	12 laptops/ 4 desktops	3rd party	N/A	$16,000.00	■		
13	Server Buyout	Buyout leased FileHold server	3rd party	N/A	$1,000.00	■		

[9] The ID's in this work plan reference to the project descriptions in the project timelines outlined in the report
[10] Annual Hosting Costs: $500.00 + Maintenance of 20% ($1,800.00)

Township of South Stormont Workplan								
Highlighted Projects Denote Shared Service Opportunity						**2018**	**2019**	**2020**
ID	**Project Name**	**Comments**	**Who**	**Effort Days**	**Annual Budget**			
14	IT Policy Development	Leverage existing policy templates and customize	SS	ongoing	$0	■	■	■
15	FileHold Training Strategy	Leverage free training (remote and onsite)	SS/3rd party	ongoing	$0	■	■	■
16	RFI/RFQ Development	MDM, Security, Network as a service	SS/3rd party	10	$7,500.00	■		
17	Building Inspection	ProWare replacement	SS/3rd party	60-90	TBD (in progress)		■	
18	Mobile Device Management	Delivered as a service (SaaS) -	3rd party	30	$7,200.00		■	
19	Managed Security Services	Recommend: Out-task this service	3rd party	TBD	$6,000.00 - $48,000.00		■	■
20	Wiki Development	Leverage O365 - Develop a formal intranet	3rd party	45	$5,000.00 - $10,000.00		■	
21	Website Development	Recommend: eSolutions[11]: (eServices)	3rd party	60	$35,000.00		■	
22	FileHold SharePoint	integrate FileHold with SharePoint	3rd party	TBD	$2,500.00		■	
23	Cloud Storage Strategy	Leverage O365 - OneDrive	SS	ongoing	$0		■	■
24	Managed Network Services	This service could include remote desktop support	3rd party	ongoing	$10,000.00		■	■
25	Digital Signatures	Select software/service	3rd party	TBD	$1,000.00		■	■
26	DR as a Service (DRaaS)	Engage a 3rd party to provide DR services	3rd party	ongoing	$5,000.00			■
27	By-Law Enforcement	Work required to research solutions	3rd party	TBD	$20,000.00			■
28	Work Order System	To be implemented once the Township develops required processes	3rd party	TBD	TBD			■

[11] eSolutions is the leader in municipal websites and will offer the Township a 30%+ discount on annual support as part of a "shared services" program within the Counties ($1,200.00 to $4,500.00 per year)

Appendix F – Mobile Device Management Options

Centralized management of mobility devices by a qualified third-party (as a service) will enable the Township to integrate and manage mobile devices within its infrastructure. At its core, every enterprise mobility solution should manage devices (even if the information is the priority, remote wipe is still important for security), manage applications, blacklist apps based on certain characteristics (high data usage for example), allow for application and authentication controls, and manage content.

Requirements can be divided into 4 areas:

- **Base Device Features (MDM) -** basic device management features provided by previous MDM solutions
- **Mobile Application Management (MAM) -** management of devices from application level, both from the Township's network and from other apps on the device
- **Mobile Identity Management (MIM) -**functions like role-based access that apply context such as geo-fencing to determine the location of device users
- **Mobile Content Management (MCM) -** oversight and control at a content level, which can include copy and paste restriction and access to business content

Key Feature List		
Base Device Features (MDM) – IT policy and profile provisioning		
Feature	Details	Notes
Self-Registration	Ability for Town staff to register for the program	
Asset Inventory	Inventory of mobile devices accessing Town applications	
Remote Configuration	Includes VPN, WiFi, Bluetooth, etc.	If ability to onboard a device to WiFi is important
Profile Provisioning (Remote)	Includes group-based policy capabilities and password enforcement	
Jailbreak Detection	Detection of rooted or jailbroken device	
Roaming Device Management	Includes ability to remotely lock the device	
Multi-profile capabilities	Allow multiple users on a single device	Having multiple users share a device
Malware Detection	Malicious app identification	
Mobile Application Management (MAM) – Centralized application delivery		
Containerization	Ability to remote wipe container	
Enterprise App Store	Ability for the Town to deploy in-house or commercial apps	
IT Controlled App Delivery	Town portal for application delivery and removal	
Monitoring	Ability to monitor application usage	
Enterprise Printing	Secure printing capabilities	Managing printers could be a nice feature
Mobile Identity Management (MIM) – Data policy provisioning		
User & Device Certificate Management	Includes authentication and single sign-on	
Geolocation	Allow the Town to track location of all devices	
Mobile Content Management (MCM) – Secure access to data		
Secure Access to Documents	Ability to distribute and access employee documents	

Appendix G – Township of South Stormont 2018 Task List (Expanded)