BLACKLINE CONSULTING

A Higher Standard

Information Technology Strategic Plan

Township of Muskoka Lakes

Final Report

22nd December 2021

PRIVATE AND CONFIDENTIAL

Contents


SUMMARY OF FINDINGS

Summary of findings

Suitable for the needs of the Township

Partial meets the needs or requires some attention

Requires more immediate attention

Item	Suitability	Observations
Business Systems 		**Some gaps in coverage and a couple of older systems needing replacement** ► Asset management, planning and work orders are areas without supporting systems. However, CityWorks has the potential to meet some of these requirements. ► One of the applications used by Public Works is no longer supported by the vendor and should be replaced. Similarly, Vadim, the finance system, is near the end of its life. ► Very few services are available online. There is little to no integration between systems. If more services are made available online, the Township will need to connect the website with operational systems.
Data Centre 		**The computer room is basic but functional, however, there is no secondary facility and equipment** ► The hardware and networking equipment has redundant components such as dual network cards in servers and two firewalls on the network. However, in the event of a disaster, there is no alternate equipment that can take over. ► Backups occur, but there is no plan on how to restore systems in the event of a disaster and no hardware to restore to.
Network 		**All staff require network and Internet access, but the current network is not resilient and has low bandwidth** ► There are a number of single points of failure that if the component failed network or Internet access would be lost. For example, each satellite location outside of Township hall has a single firewall and single connection to the Internet via Township hall.

Summary of findings

Suitable for the needs of the Township

Partial meets the needs or requires some attention

Requires more immediate attention

Item	Suitability	Observations
Infrastructure 		**Virtualized Windows servers is a good practice** ► The Township runs three physical servers that support 22 virtual servers. The Township predominately uses Windows Server 2016 but still has 8 virtual servers running Windows Server 2012 R2. Microsoft will cease support for this operating system in 2023. ► The Microsoft Exchange email server is hosted on-site, but email is received by the Sophos firewall and relayed to the Exchange server.
Governance 		**Decision making for IT is decentralized** ► Each department at the Township makes decisions about its own needs and will typically procure software directly from the vendor. ► In the absence of anyone internally making decisions about IT and setting policies, the managed service provider has taken on some of this task. For example, they set the blacklists for spam email and for websites, barring staff from visiting them.
Organization 		**Some IT activities are not completed today** ► The contract with the managed services provider is limited to supporting the hardware and networking. ► With no IT staff at the Township, many normal activities that an IT function would conduct are not completed, including helpdesk, upgrades, security management, disaster recovery and project management. ► With past changes to the service provider and Township staff, no one person has a clear understanding of all elements of IT at the Township whether that is vendors, contracts, software and versions, location of equipment etc.

Summary of findings

Suitable for the needs of the Township

Partial meets the needs or requires some attention

Requires more immediate attention

Item	Suitability	Observations
Budget 		**The operating budget is in line with other municipalities** ► The Township spends approximately 2% of its operating expenses on IT, which is near the lower end of the range we see at other Ontario municipalities, but certainly within the range. ► The capital forecasts emphasizes the Township does not have specific plans for IT in future years.

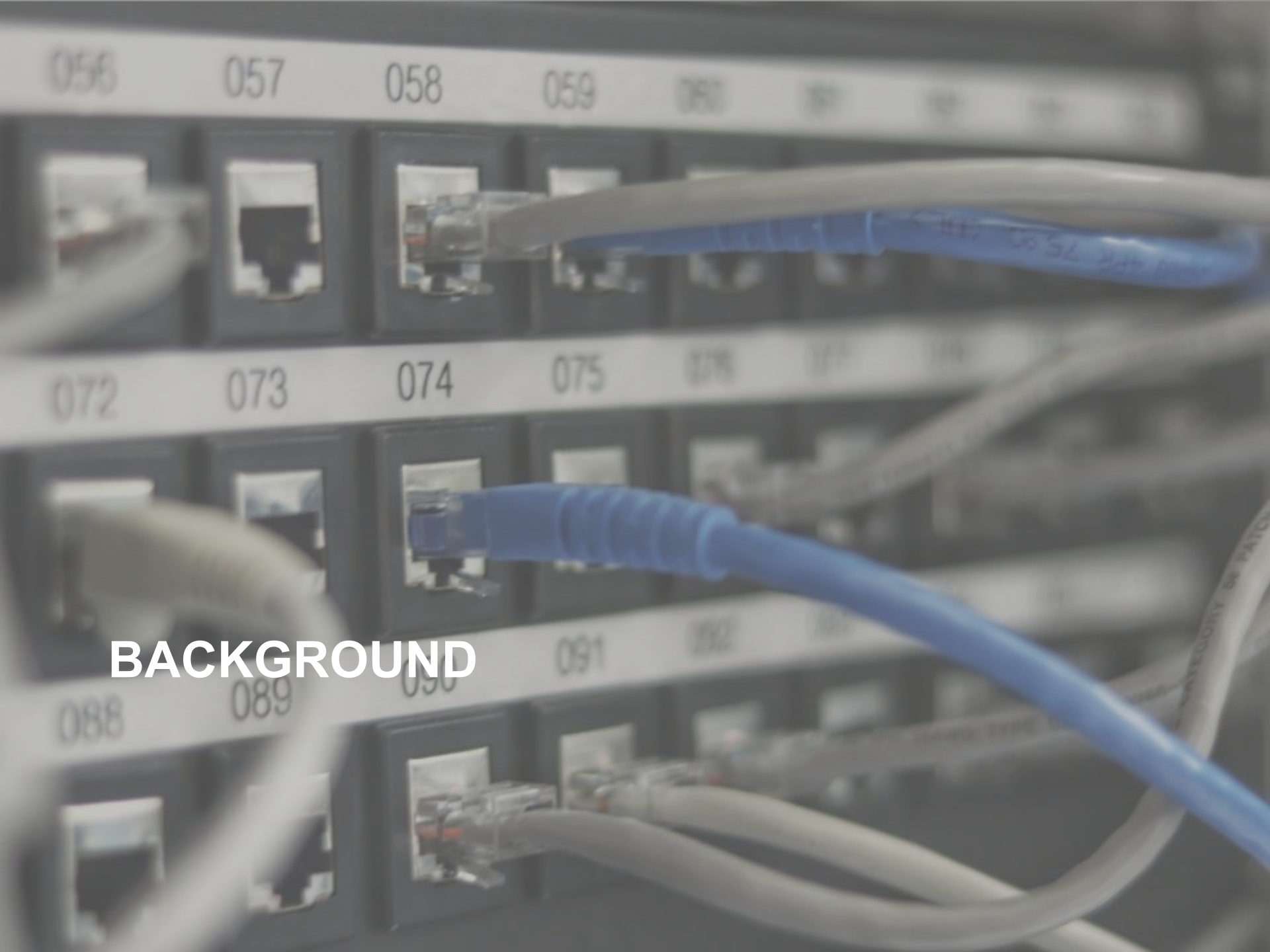
Recommendations

Drawing upon our findings, staff input and the strategic plan, we have identified 15 specific recommendations

We have grouped our recommendations under three pillars that explain the objective of this IT strategic plan.

- To be successful with this plan, the Township will need to hire a knowledgeable IT resource.

		# Recommendation
Reinvent the Resident Experience	Recent experience has emphasized the benefits of offering services digitally and online. To expand the online offering, the Township will need to enhance the capabilities of the existing website, ideally, creating a portal that residents can log into to access Township services and see a history of their interactions.	1. Create portal 2. Migrate services 3. Add payment capabilities 4. Market to residents 5. Connect to operational systems
Automate Business Processes	A number of the current systems do not meet the needs of the Township and should be replaced. Additionally, there are processes that do not have good system support that would benefit from automation and technology.	6. Finish current projects 7. Migrate to Office 365 8. Replace the finance system 9. Establish workflow, approvals and digital signatures 10. Implement an HR solution 11. Eliminate paper time recording
Upgrade the IT Capabilities	After you establish your next managed services agreement, work with the provider to upgrade aspects of the IT infrastructure to enable more advanced capabilities.	12. Fibre broadband Internet connection 13. Review site connection speeds 14. Review the phone systems 15. Investigate mobile technologies for staff that are mobile


BACKGROUND

This report presents Blackline's assessment of the current IT systems and services at the Township

Background

In 2021, the Township of Muskoka Lakes (the Township or Muskoka Lakes) selected Blackline Consulting (Blackline) to assist you to develop an information technology strategic plan.

The project will assess the current IT environment, consider what needs the Township has for technology, consult peers and ultimately develop an IT strategic plan.

Approach

We gathered the information presented in this report from interviews with Township staff, third-party providers and reviewing available documentation.

Our proposal contained a four-phased approach to ultimately deliver an IT strategic plan

The graphic below provides an outline of our approach.

- This report reflects the output from all four phases of our work.

Phase One – Environmental Assessment

Gathered documentation and interviewed staff and the Townships IT service provider to get a perspective of the IT environment.

Phase Two – Needs Assessment & Environmental Scan

Consulted peers to understand their position relative to IT and the reasons for the decisions they had made.

Phase Three – Cybersecurity and Risk Assessment

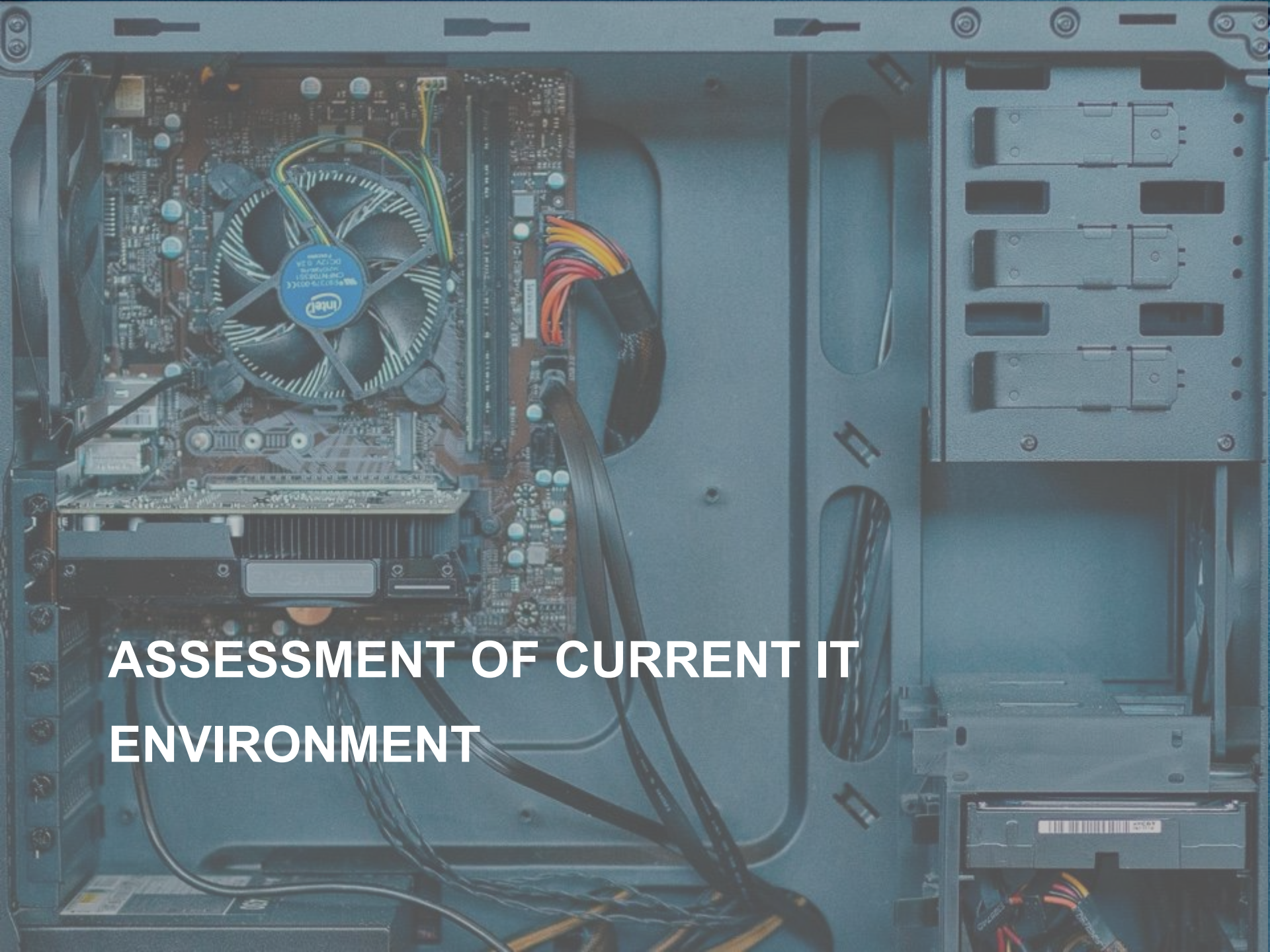
Used the NIST cybersecurity framework to assess the preparedness of the Township in the event of a cybersecurity incident.

Phase Four – Final Report

Created a final IT strategy that lays of the direction for IT at the Township.

Glossary

Acronym	Definition	Acronym	Definition
CapEx	Capital Expenditure	**PC**	Personal Computer
CRM	Customer Relationship Management	**PIA**	Privacy Impact Assessment
DC	Data Centre	**PM**	Project Management
DMZ	Demilitarized Zone	**RFP**	Request for Proposal
EUE	End User Equipment	**SaaS**	Software as a Service
FTE	Full-time Equivalent	**SAN**	Storage Area Network
HRIS	Human Resources Information System	**SLA**	Service Level Agreement
IaaS	Infrastructure as a Service	**SME**	Subject Matter Expert
ISP	Internet Service Provider	**SPOF**	Single Point of Failure
MS	Microsoft	**TCO**	Total Cost of Ownership
MSA	Managed Service Agreement	**VLAN**	Virtual Local Area Network
OS	Operating System	**VOR**	Vendor of Record
OpEx	Operating Expenditure	**VPN**	Virtual Private Network
PaaS	Platform as a Service		



ASSESSMENT OF CURRENT IT ENVIRONMENT

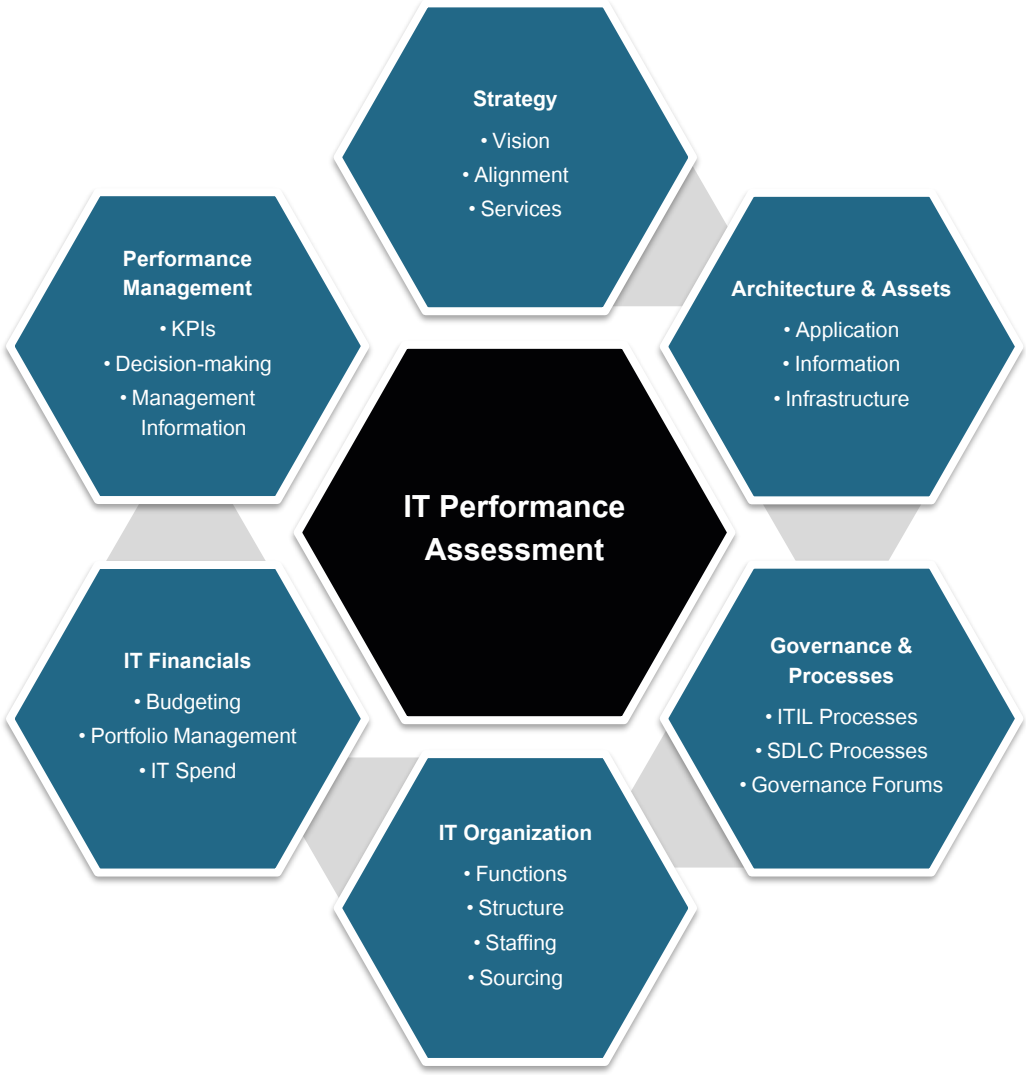
We applied our comprehensive IT assessment framework

Blackline's assessment of the Township followed the assessment framework illustrated to the right

The following pages provide our observations and assessment of each of the six domains, with the exception of:

- **Strategy** – as this project is intended to develop the IT strategic plan
- **Performance Management** – limited data is kept on IT

For each domain, we describe what is in place and indicate whether that is adequate and reflective of common practice.

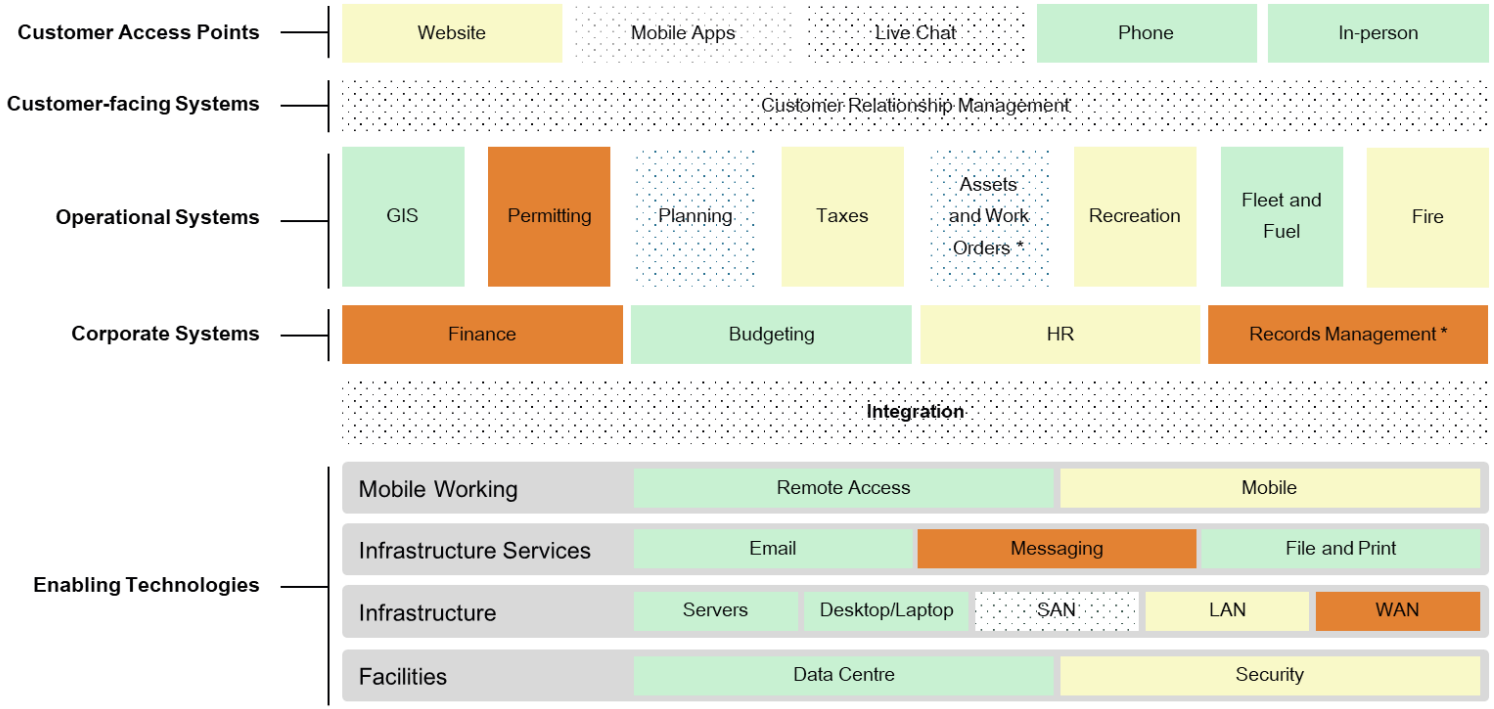


Business systems

The diagram below shows a logical architecture of a municipality

It shows the common systems municipalities run. We have coloured them to show where the Township stands using the following definitions:

- Fully meeting your needs and current
- Partially meeting your needs or needing updates
- Not meeting your needs or having reached end-of-life
- No system support
- On the following pages, we elaborate on our ratings.



* Projects are underway to implement new systems to support these function

No one has a full view of all the business systems used

Each department concerns itself with just the software they use

Any organization should have at least one person who is thinking about all of the software used for a number of reasons.

- At purchase – they consider whether the functionality sought exists in another system already owned; whether the software meets security standards; whether it will adversely affect any other systems; whether it runs on the operating systems used.
- During implementation – they consider whether it may need to connect to other systems.
- After implementation – they consider whether upgrades are required.

For this report, we gathered an index of business systems (contained in Appendix A) from interviews and reviewing available invoices and software contracts.

- Few details of the versions of the applications were available. We consider this a key piece of information as it tells us whether the Township is using the most current version of a piece of software.
- Running older versions can incur a number of problems:
  - You cannot upgrade hardware as the software does not support the new hardware
  - You cannot upgrade operating systems as the software does not support the new OS
  - The vendor stops supporting the software

There is limited application integration between the municipality's systems

Integration is connecting different IT systems so that they can share data.

- Although there is a desire for increased integration amongst the various departments, little integration exists today. Not having integration tends to increase data duplication and the likelihood of errors and omissions.

Some of the existing systems do not fully meet the Township's needs

Two systems appear to only partially cover the functionality the Township needs:

- Recreation: use BookKing.ca, but this only supports facility booking. Skate and swim programs, for example, do not appear on the BookKing.ca webpage.
- HR: HRWize is a Cloud-based HR system. The Township uses it for recruitment, but because of privacy concerns, is not using the employee management functionality.

Additionally, three systems are candidates for replacement:

- Website: the Township wishes to be able to offer a full set of digital services, which it cannot do with the current website.
- Finance: iCity from Central Square is used by a range of municipalities in Ontario. Many highlight limitations, including difficulty getting data from other systems into the software, dated user interface, no recent upgrades to functionality and not operating on more recent Windows OS.
- Permitting: Land Information System Application (LISA) supports building permit applications and many staff use it to understand the history of properties. It does not support the other permits and licenses the Township issues.

Planning, asset management and work orders do not have systems to support their processes

The Township is in the process of implementing CityWorks to address the work order and asset management functionality.

- We also highlighted the Township does not have integration between the systems to exchange common data.

Less of a concern is not having a CRM

However, if the Township does move towards more digital services, a CRM will become more important - as will integration.

- If a resident wants to request a service online, that request needs to get to the right staff member. For example, if a resident reports a pothole through a digital channel, that report needs to create a work order potentially in CityWorks.

Few services are available digitally

The Township has an extensive website covering all of its services

We surveyed the website and identified the following services as available online:

Area	Online Service
CivicWeb	Access to Council calendar, agendas and minutes
Report a concern	Online form to report a matter to the Township
Burn permit	Online form to apply for a burn permit
Facility rental	Online form to inquire about facilities
Change of address	Online form to register a change of address
Tax Portal	Registration system to view transaction details of your property tax account and to make payment by credit card via a third party
Recruitment	Online portal to register and apply for positions
Engage Muskoka	Online service to gather resident input on community decisions – provided by BangTheTable

There are a larger number of services where forms can be accessed on the website but must be submitted manually

- PDF forms come in two formats – fillable and non-fillable. Fillable forms allow the resident to type text directly into fields in the form and save the completed form, which can be emailed (or printed). Non-fillable require the resident to print the form, fill it in by hand and then mail or physically deliver.

Form Type	Service Area
Non-fillable	▸ Heritage designation ▸ Licenses and Permits (over 15) ▸ Roads permits (5) ▸ Building permit applications (3)
Fillable	▸ Fire permit applications (4) ▸ Pre-authorized payment ▸ Planning applications (8)

To provide digital services would require extensions to the current website

Firstly, more online forms to capture requests. Next workflow to route requests and seek approvals, then integration with operational systems to execute the service request.

- The next level of sophistication is for residents to have accounts to log into and to see the status of requests and their history.

The website is hosted by a third party, but the Township still has the responsibility to maintain it

The main website is hosted by eSolutions in Waterloo

eSolutions are a common provider of website services to municipalities.

- However, they will not generally maintain content, registrations, search rankings or other aspects of running a website – those activities remain something for the Township to do.
- The effort required to maintain a website should not be underestimated. As municipal services change, websites have to be updated to reflect current information.
- A former employee is listed as the domain name administrator for Muskokalakes.ca – which is due for renewal before June 2022. This should be updated to ensure that reminders go to current staff to renew. The Township should instigate a process when staff leave that ensures these sorts of administrative contacts are updated.
- The Township has a page hosted by BookKing.ca to rent facilities, however, we could not find a link from the Township's website to this booking page and none of the functions on the BookKing page worked.

There are over 60 separate service web pages on the website.

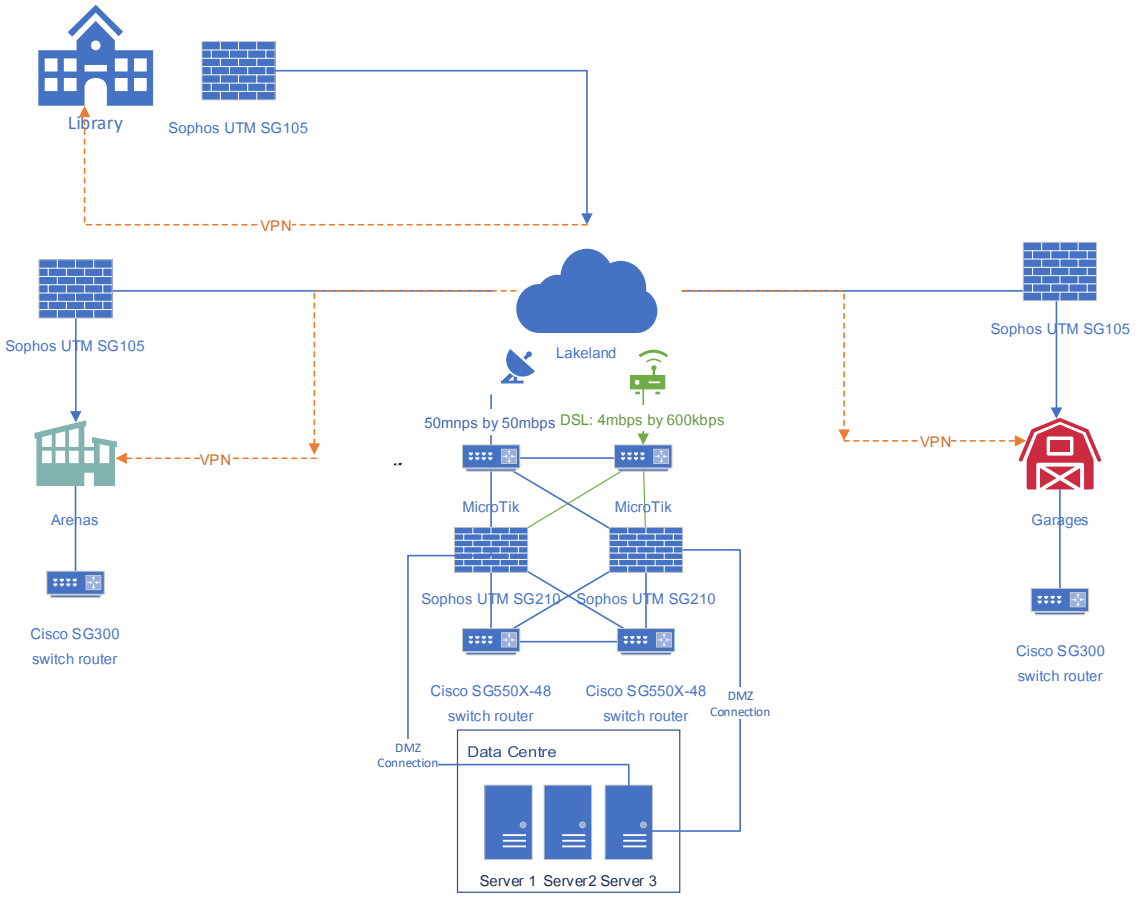
- Every page has a separate contact number and many have faxes listed. In previous experiences, we have heard directly from residents how this situation makes accessing Township services more confusing and difficult to get to the right place first time.

Internet connectivity to Township offices is limited

The Township has a primary and backup Internet connection from Lakeland

At 50Mbps, the primary connection is adequate for the size of the staff, but as a wireless connection can be affected by weather.

- The secondary is a DSL connection that has a very limited upload bandwidth. In the event of a failure of the primary connection, it is unlikely that this would provide a seamless backup. Additionally, staff working remotely would likely not be able to access the servers.
- Having both connections from the same service provider poses the risk that an incident at Lakeland could take out both lines.
- Single firewalls exist at most sites, with Township hall having two firewalls. As well as preventing unwanted external network traffic from entering the Township, the firewall also restricts which websites staff can visit.
- Staff commented that access to many websites is blocked – apparently, the managed services provider has set this policy. One example was the Google Suite that was required to be able to collaborate with certain third parties.



Without highly reliable Internet connections, the Township's IT options will be limited

Fibre Internet connections typically have a higher bandwidth and are more reliable

Fibre in less populated area's of Ontario can be limited, which is the case in the Region.

- A high speed, reliable Internet connection is more important today than ever, for a number of reasons:
  - Many software applications used by municipalities are moving to Cloud-only configurations – the Township has recently implemented Questica, which is an example where it was only offered as a Cloud option. Without a reliable connection, staff working from the office will not be able to use Cloud-based software.
  - COVID led many staff to work remotely and it seems that many organizations will move to a hybrid model – some remote and some on-site work. Without a reliable connection, remote staff will not be able to access on-site IT services
  - Offering digital services to residents will increase the information sent to the Township..

Many projects are underway across the province to try to rectify this.

- The District has formed the Muskoka Economic Recovery Task Force, which is prioritizing getting broadband services for the whole region. This will be years before coming to fruition.
- Regional broadband is very likely the best solution for the Township, in the long run, however, it is still worthwhile evaluating whether the Township can cost effectively implement an independent solution in the interim.

The computer room is basic but functional

The Township has one computer room located on the lower level inside the Township's office

The computer room is basic and meets the immediate needs of the Township, but it does have some limitations.

- The positive elements include a security keypad to restrict entry, an independent dedicated air conditioner and a ceiling suspended cable management tray.
- All server and network equipment is mounted correctly in a data centre racking unit shown to the right. Each of the components has been configured with redundancy including dual power, dual UPS and dual network cards in the servers. If any of these components failed, the second component can take the workload so there is no interruption of service.

The Uptime Institute defines how frequently a computer room will experience an outage based on a set of characteristics that reduce the frequency and severity of an outage. Using these characteristics highlights some of the limitations of Muskoka's situation.

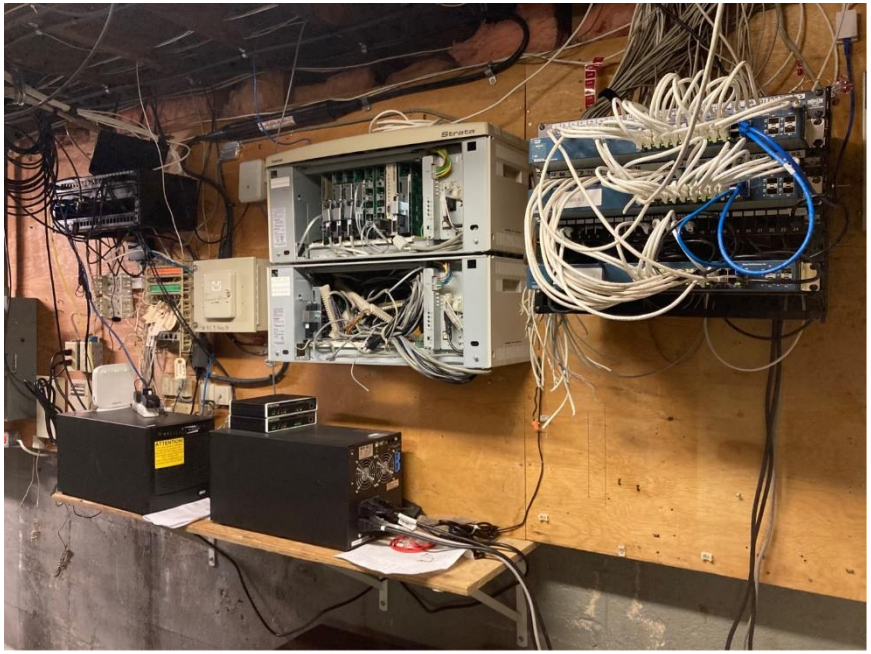
- Fire suppression – the risk of fire has been considered with a fire extinguisher mounted on the wall – however, it is located on the far side of the room, making it largely unusable in the event of a fire.
- Location – being on the lower level increases the risk of damage from a flood. This is commonly mitigated by installing a 12" raised floor, however, the ceiling height in the computer room will not allow this.

An adjacent electrical room does not meet the same standards

Much of the network patching panels and the Township's Internet connection are located in the adjacent electrical room

This room does not have air conditioning and is not suited to housing computer equipment.

- The image to the right shows those patch panels and two black UPS.
- The large grey boxes mounted on the wall are the old phone system, which has been abandoned and not removed.



Having the servers located in your main office has advantages and disadvantages.

- It allows staff working in the office to have good network access to the servers and fast response times. However, with the limited Internet connectivity, anyone working outside the office may have difficulty accessing the servers.
- This is a particular concern with the current pandemic working conditions with most office workers working from home.

Recovering IT systems from a disaster would likely take over a week

The managed services provider completes backups for the Township

A set of backups are kept on-site and a second set at the managed services provider. If a disaster befell the main office, the off-site backups would be available.

- The managed services provider has tested restoring the backups previously, but as staff at the Township changed, this practice has been discontinued.

This practice is suitable to restore accidentally deleted files but is insufficient to restore IT operations following a more substantial disaster

In the event of a disaster affecting IT systems, the Township is missing two key components to enable it to restore operations quickly.

- The Township does not have a Disaster Recovery Plan (DRP). A DRP outlines how to restore IT systems after a disaster. While it is still feasible to restore operations, organizations find it takes much longer without having planned and practiced.
- The Township has conducted a rudimentary prioritization to highlight which systems are more urgently needed by a department.
- The second issue is the Township has no secondary location or alternate hardware to restore the backups to. In the event of a material disaster, such as a loss of the data centre through a fire or flood, the Township would have to procure hardware, find a location to house it, begin the process of restoring systems and reconfigure the network for the new server locations. This process could take anywhere from 5 to 20 days.

The managed service provider has indicated that they would offer assistance in the event of a disaster

This assistance is not specified in the contract and the Township would be acting in good faith to rely on it.

- In verbal conversations, the managed services provider has indicated that they would have hardware available to restore Township systems to.

COVID forced the Township to refresh many of its user devices

The Township does not follow a defined refresh cycle for its user computing devices

It is common practice to set a budget for user computers that allows them to be replaced in a specified number of years, say three or five years.

- When staff had to work from home, the Township replaced many devices with laptops to make the transition smoother. While there has been a material refresh, there may still be some older devices.

The Township has installed a VOIP telephone system that represents common practice.

- We understand that the telephony system also includes a messaging platform, but it is not used by all staff. It is not clear whether this is due to not being aware of it, having a preference for another platform or limitations in the functionality.
- Working remotely has increased adoption, but we understand that tools such as Zoom and Microsoft Teams are also used, but inconsistently.

Staff are able to access the Township IT systems remotely

Most staff use Sophos VPN to connect to the Township systems from a remote location, using their Windows username and password.

- The Township also operated a Parallels server remote application server to access some applications.
- Finally, some of the IT vendors are able to gain remote access to perform maintenance on their applications. For example, iCity (Central Square) uses an unattended application, which is installed by the managed services provider when requested and removed after the maintenance is complete.

The various other municipal sites use VPN connections to access the IT systems.

- Five sites (Bala Arena, Port Carling Arena, Bala Library, Glen Orchard Garage and Port Carling Library) use a site-to-site VPN. This is a permanent connection that uses the site's Internet connection to access the main office as though it was connected to the network.
- The remaining 19 sites use wireless connections to access IT services, a mix of LTE and 900Mhz, which is similar to how mobile phones access the Internet.
- Finally, the District has a site-site VPN to allow them to access the GIS and SQL server that runs MAPINFO and ESRI applications.

Governance of IT, simply put, is making decisions about IT systems and processes

The diagram to the right is Blackline's model for IT governance

We believe that each of the bodies shown should exist in some form for effective governance and decision-making.

- Each body does not need to exist independently, it should just be clear who is making which decision.

✓ indicates the Township has this component

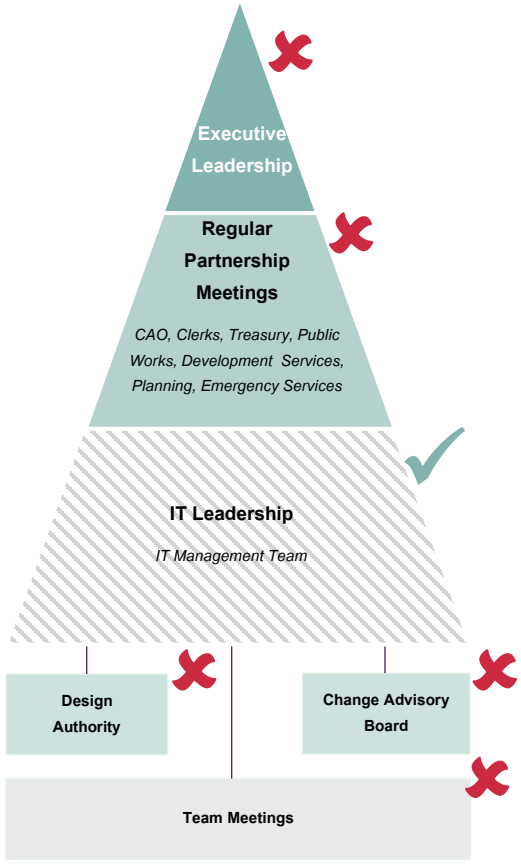
✗ indicates the Township does not have this component

The Township has executive leadership meetings, however, IT is not a formal part of the agenda

With the outsourcing of IT, there is no need for the Township to have IT team meetings.

- The Township has maintained a designated staff member who has responsibility for IT, which we have classed as IT leadership. The role predominately liaises with the managed services provider.
- Commonly another role of IT leadership is facilitating the partnership meetings – having departments discuss their needs for IT and establishing corporate priorities.
- The final real area of concern is Design Authority – deciding on the specific technologies the municipality will use and the policies it will adopt – such as security.

Core IT Governance Forums



- Formal governance structure that includes the Senior Leadership Team
- Prioritize departmental needs
- Discuss IT service performance
- Status of existing projects
- Develop multi-year strategic plan, and operational plans
- Monitor progress against plans and IT performance
- Control design (fit for purpose), Control stability
- Forum for communication with IT staff

No criteria are in place for selecting suitable Cloud providers

As we have indicated in the architecture section, the Township has a number of Cloud-hosted solutions already

The Township does not have a policy that guides what qualifies as an acceptable Cloud solution.

- HRWize presents a practical example. The company hosts its platform in the UK. The managed services provider has advised that no confidential data should be stored in this system as the data would reside in the UK, so no employee records are in this HR solution.
- The Government of Canada's position, and the current privacy legislation PIPEDA, is that Canadian organizations remain responsible for the data and that contracts with third parties should offer equivalent protections.
- Since Muskoka Lakes does not have policies on working with Cloud providers, these measures are not in place and the system is not being used for its intended purpose.

The Township does not have IT staff

The Township previously received IT services from the District

In 2017, the Township selected the managed services provider to replace the service provided by the District.

- While with the District and now with the managed services provider, the Township has relied on staff that are no longer with the Township and it seems that institutional knowledge related to IT has been lost.
- The table to the right gives some definition of the various levels of support that are required to run an IT function.

The Township does not have easy access to key administrative elements of IT

With the change of staff and responsibilities, it was difficult for staff to track down information. Key items that the Township should ensure it has in its possession include:

  - Support agreements
  - Licenses
  - Administrator log in account details
  - Documentation of the current environment
- The absence of documentation on the current environment made conducting this review more difficult, forcing us to attempt to discover the software, hardware and configurations through inspection and interview.

Level	Function	Support methodology
Tier 0	Self-help and user-retrieved information	Users retrieve support information from the web and mobile pages or apps, including FAQs, detailed product and technical information, blog posts, manuals, and search functions.
Tier 1	Basic help desk resolution	Support for basic customer issues such as solving usage problems and fulfilling service desk requests that need IT involvement.
Tier 2	In-depth technical support	Experienced and knowledgeable technicians assess issues and provide solutions for problems that cannot be handled by tier 1.
Tier 3	Expert product and service support	Tier 3 technicians attempt to duplicate problems and define root causes, using product designs, code, or specifications. New fixes are documented for use by Tier 1 and Tier 2 personnel.

Many essential IT functions are not covered at the Township

The scope of the contract with the managed services provider is limited by design

Since the Township has no IT staff, this leaves gaps in the activities that should be happening.

- For example, the contract states that tier 1 support should be supplied by Township – when a user has a problem, tier 1 is the first person they should contact.
- The Township has no staff to provide this support, so the managed service provider accepts incidents reported to them via email.
- While backups are completed, the current contract does not cover recovering from a disaster.

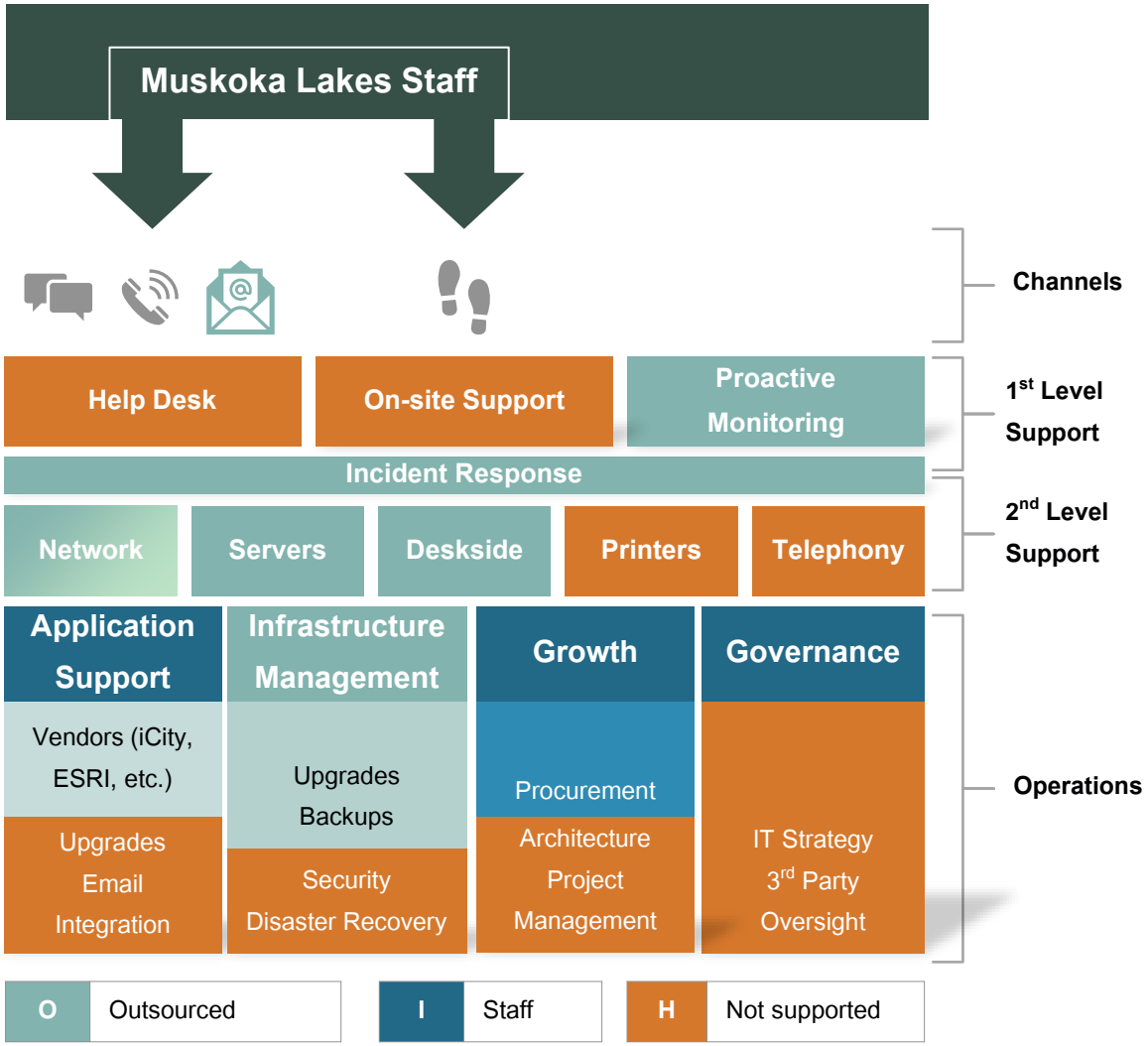
The Township relies on software vendors to provide support to its applications

The Township may not realize this is the case.

- No contracts were available to confirm this is formalized with vendors.

There is no IT project management

In its absence, both the CityWorks and mFiles implementations have been delayed.

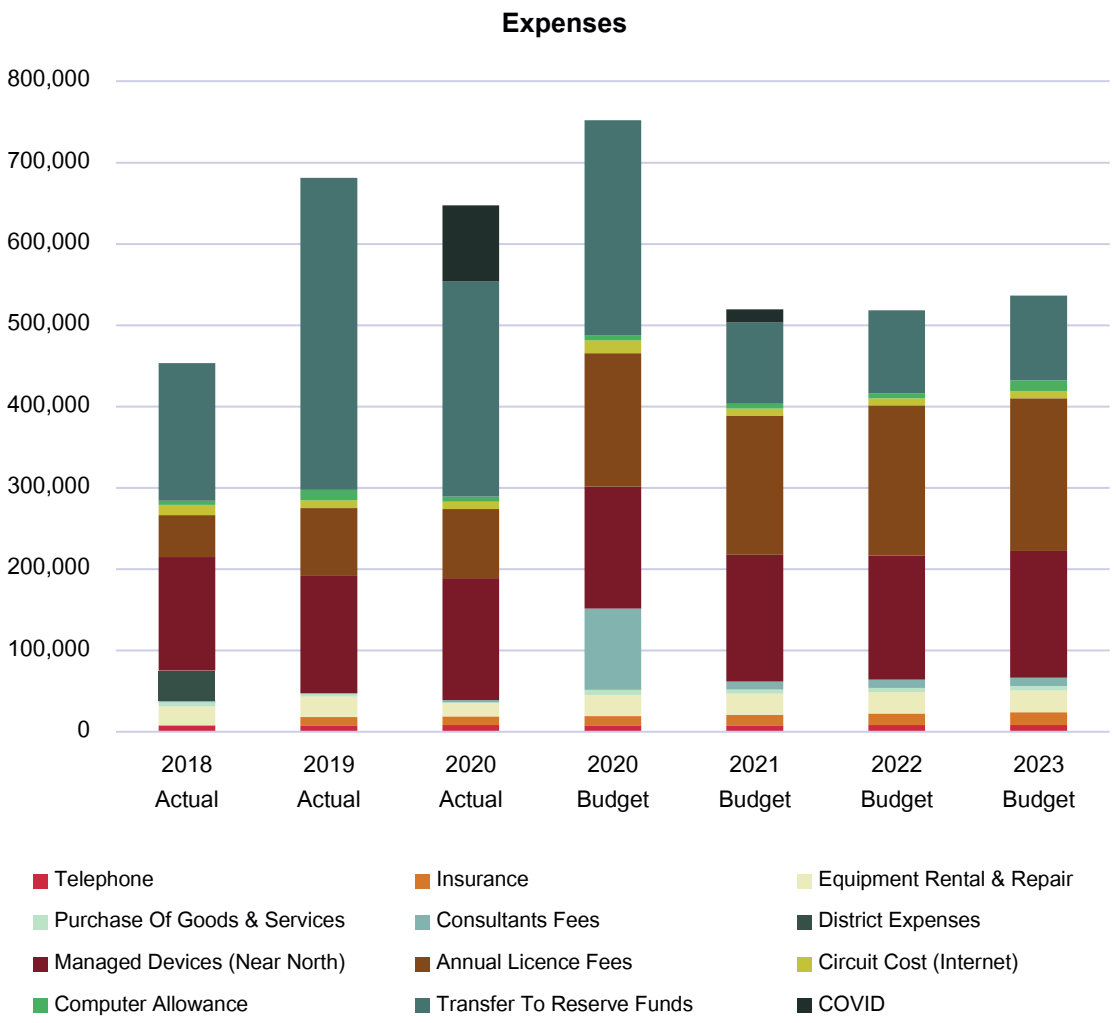


The Township's IT budget is in line with benchmarks

On average, IT operating spend as a percent of the Township's total operating expense is 4%

Benchmarks are typically between 1.2% and 9.1%, with a cross-industry average at 4.3%.

- Our experience with Ontario municipalities shows spending more commonly of between 1-5%. If we remove the Transfer to Reserves, which in effect is equivalent to depreciation – the Township expense approaches 2%, again in line with common practice.
- Typically, Personnel & Benefits would represent between 40-45% of IT operating expense and Services would be 20-30% (depending on the level of outsourcing). However, the Township does not have any IT staff and outsourcing on average represents 26% of the IT budget.



Beyond hardware refresh, there are few IT costs forecast in the future

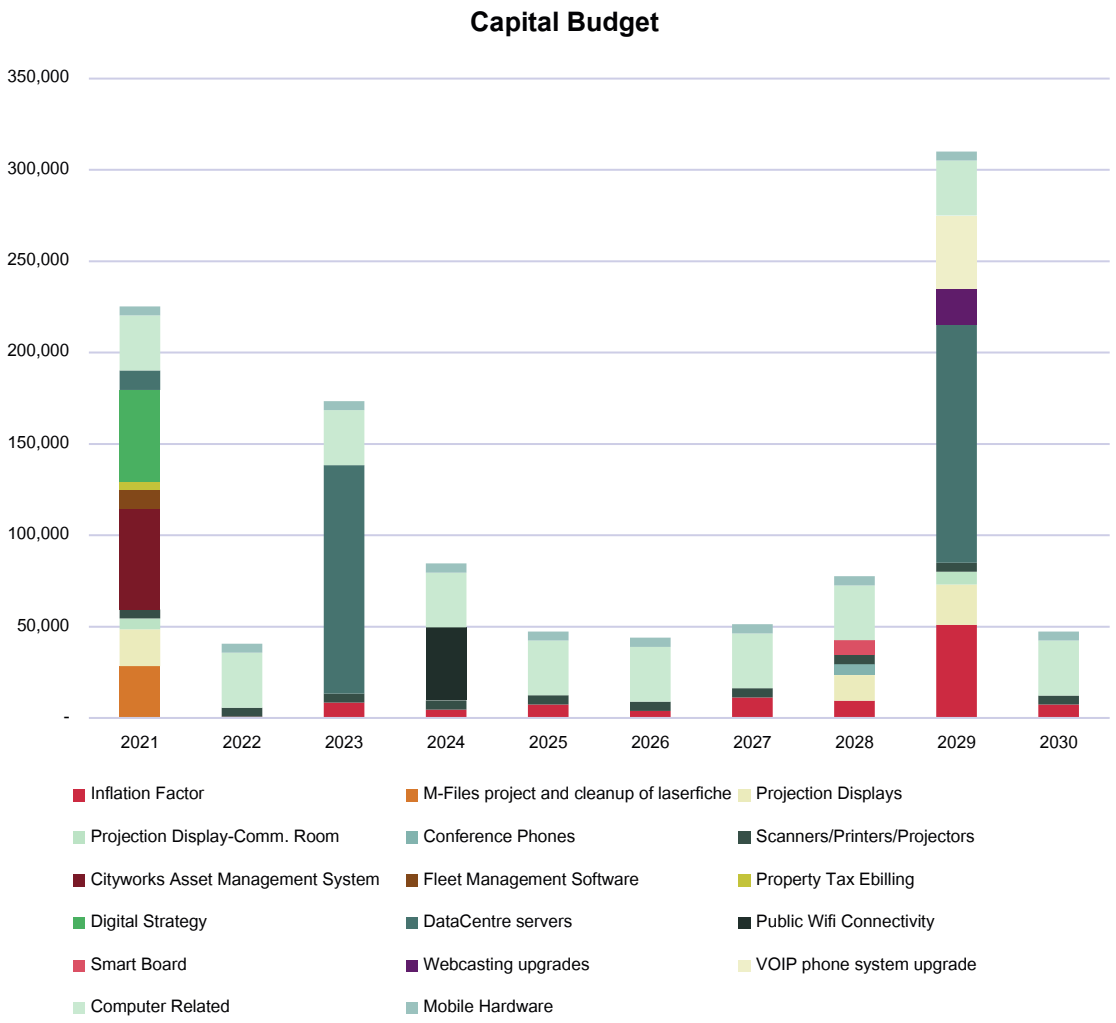
The Township has a ten-year budget for IT

The majority of the budget in this forecast relates to computer and server replacements.

- At around $266k over the next 10 years, data centre services represent 24% of the overall capital costs while computer costs represent 27% at $300k.
- The two active projects, mFiles and CityWorks, have budgets in 2021, but little has been identified in future years.

The budget emphasizes that Township does not have an IT strategic plan.

- The IT strategic plan that comes from this project will identify IT projects that the Township should be undertaking, which in turn should have a budget associated with them in future years.




PEER CONSULTATIONS

Report Context

Background

The Township of Muskoka Lakes (the Township) is developing a new Information Technology Strategic Plan (ITSP). As an input, Blackline Consulting (Blackline) conducted a peer study to gain an understanding of IT service delivery models and priorities at other municipalities, their network systems, application utilization and integration, and cybersecurity practices.

Approach

Blackline worked with the Township to identify twelve questions of interest. Blackline then met with representatives from the ten other municipalities listed to the right to gather their feedback.

- We gathered information through interviews with representatives, which we used to create this report. Beyond the interview, we have neither adjusted nor fact-checked the information provided.

Objective of this Report

This report compiles the input received from the participating municipalities and presents Blackline's observations and insights regarding the similarities and differences.

We thank all participants for being open and forthcoming with the information we requested in during our discussions.

Participants

The following municipalities participated in this peer study:

Gravenhurst

Huntsville

Muskoka Lakes

Georgian Bay

Bracebridge

Lake of Bays

District of Muskoka

Wellington North

Blue Mountains

Parry Sound

Saugeen Shores

Participant Characteristics

	Georgian Bay	Lake of Bays	Muskoka Lakes	Parry Sound	Blue Mountains	Wellington North	Gravenhurst	Saugeen Shores	Bracebridge	Huntsville	Muskoka District
Municipal Tier	Lower Tier	Lower Tier	Lower Tier	Single Tier	Lower Toer	Lower Tier	Lower Tier	Lower Tier	Lower Tier	Lower Tier	Upper Tier
Region	District of Muskoka	District of Muskoka	District of Muskoka	Parry Sound District	Grey County	Wellington County	District of Muskoka	Bruce County	District of Muskoka	District of Muskoka	District of Muskoka
Population	2,499	3,167	6,588	6,408	7,025	11,914	12,311	13,715	16,010	19,816	n.a.
Households	1,131	1,455	2,914	2,926	3,271	4,682	5,014	6,025	6,734	8,111	n.a.
Municipal Staff (FTE)	44	50	95	80	167	64.5	81	80	66	120	440
IT Service Delivery	Third Party	Third Party	Third Party	In House	In House	Third Party	District	In House	District	In House	In House
Municipal Operating Expenses	$8.2m	$7.5m	$15.4m	$32.2m	$28m	$16.2m	$23.4m	$29.8	$22.9m	$26.6m	$101.5m
IT Operating Expenses	$227k	$159k	$297k	$330k	$728k	$103k	$406k	$193k	$427k	$450k	$2.3m
IT OpEx (% of Municipal OpEx)	2.8%	2.1%	1.9%	1.0%	2.6%	0.6%	1.7%	0.6%	1.9%	1.7%	2.3%
IT OpEx per Municipal Staff	$5,160	$3,180	$7,828	$4,125	$4,362	$1,597	$5,012	$2,412	$6,467	$3,750	$5.241
IT OpEx per Resident	$90.85	$50.21	$45.08	$51.50	$103.70	$8.65	$32.97	$14.07	$26.66	$22.71	n.a.

Source: This data is a mix of publicly available FIRs and peer-provided, the latter was not verified by Blackline.

Six of the peers exclusively use third parties for IT services

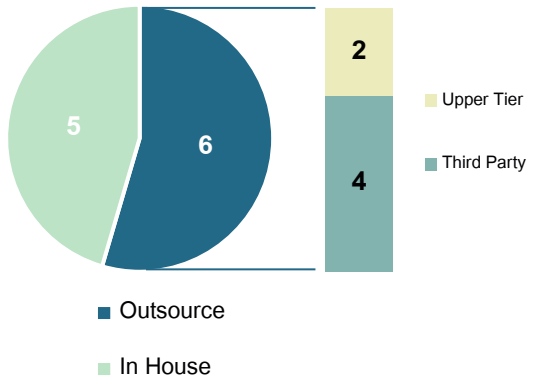
Insights

- It is common practice for municipalities and other organizations to outsource or hire third parties for their IT Operations.
- This may be for a variety of reasons, including not having sufficient capacity and resources in-house to provide all IT services.
- However, outsourcing to a private third party is not the only way these can be addressed. Through our work with other municipalities, we have found that greater collaboration with other municipalities to deliver IT services can reduce the IT operating expenses through economies of scale, negotiating power and volume discounts for IT hardware and software purchases.
- When assessing your current IT services model, consideration should be given to collaborating with neighbouring municipalities to reduce overall costs.

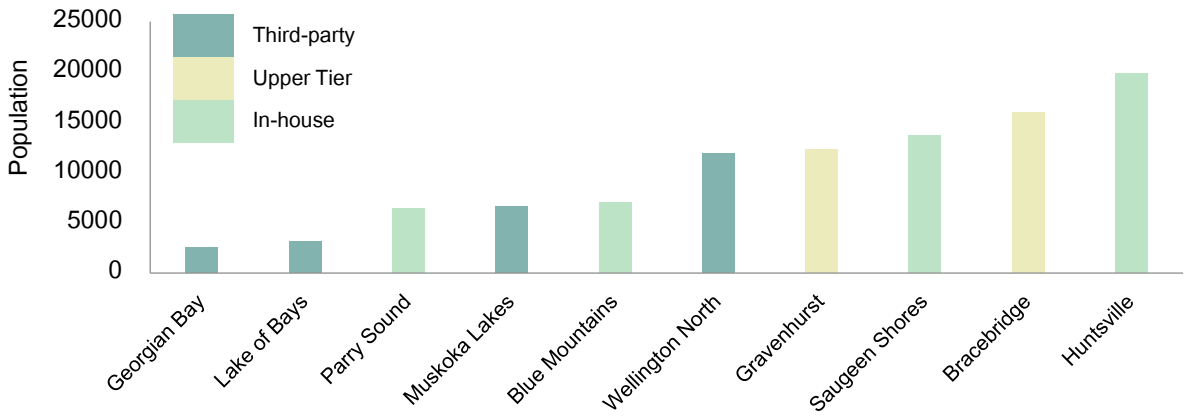
Two of the peers outsource to their upper-tier

As it's their upper tier, there already is an ongoing relationship, which has allowed them to work effectively together. As it's a government entity, it has to work with municipal systems similar to the lower tiers. This has allowed the upper tier to focus on building out a comprehensive IT function, and the lower tiers can focus on delivering resident-facing services.

IT Service Delivery



The size of the municipality is not a deciding factor for using a third party, as shown in the graph below



If outsourcing IT to a third party, municipalities should ensure they have internal capabilities for strategic support

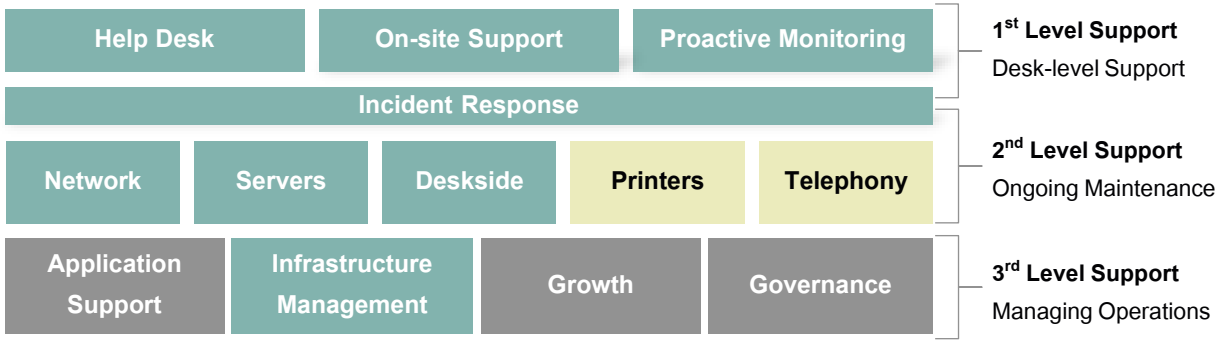
Insights

- The peers that rely heavily on third parties do not have any internal full-time IT staff. This leaves gaps in the activities that should be happening, specifically with strategic or project management support.
- For many, IT projects are out of scope for their third parties. Instead, these municipalities will either go to market or provide the third party with a separate quote outside of their contract. Only the two peers that contract to their upper tier have project management and strategic support included.
- While the bulk of IT services are provided by a third party, it is crucial to have in-house capability for growth and governance. These functions are critical for an organization to innovate, continuously improve and stay ahead of technology trends.
- Many of the peers rely on software vendors to provide support for their applications.
- When it comes to infrastructure management, most of the peers' third parties provide upgrades, backups and disaster recovery.

The peers differ in the services they contract and how they receive them

For example, one of the peers contracts an IT provider to work at the municipality one day a week.

- The diagram below highlights key IT functions. Those highlighted in blue are what many of the participating municipalities are outsourcing. Examples of specific activities include help desk resolutions, remote support to users, automated patch management, reporting on network health and patch compliance, server management and backups and network management and new installation
- IT functions highlighted in yellow are those that were not mentioned by the peers to be provided by a third party, however, these are common functions that third parties provide.
- Those in grey were also not mentioned by peers. It is uncommon for these high-level and strategic services to be provided by a third party. Rather these are services that an organization should be capable of providing.



The peers differ in their IT spend as a share of their total municipal operating expenses

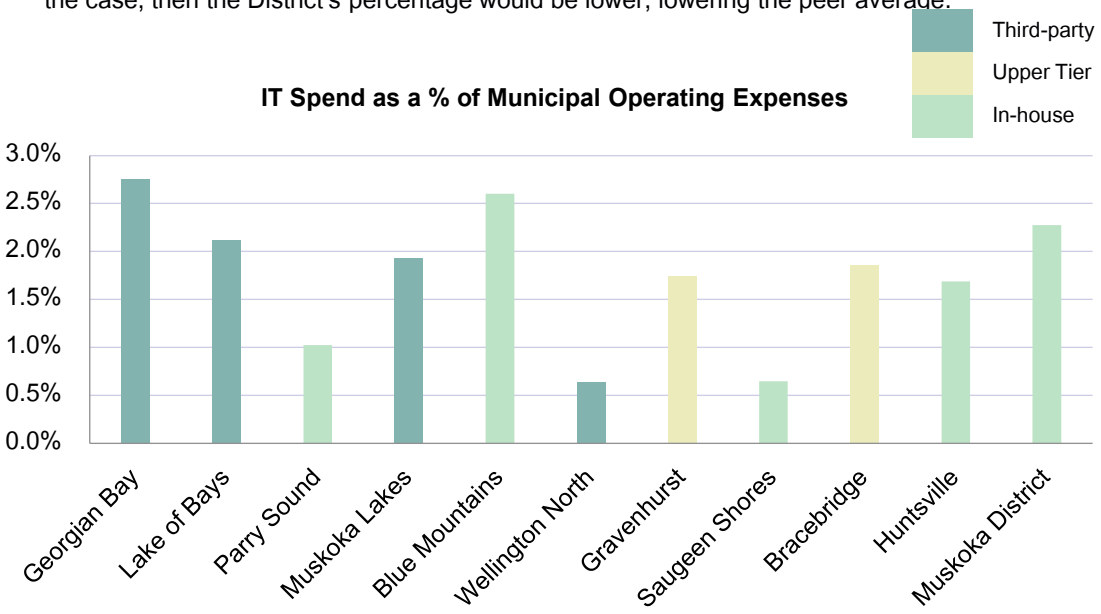
Insights

- Outsourcing IT has a small impact on the amount spent on IT as a percentage of total spend. On average, the peers using third-parties spend 2% of their municipal budget on IT, while those with in-house spend 1.6%.
- In our experience with over 60 Ontario municipalities, the range of IT spend to total municipal budget is 0.5-3%, with an average of 1.85%.
- While the average of the peers from the current study is well within this range, there are risks associated with having a low IT OpEx, mainly that IT innovation may fall behind, making it difficult to modernize technology.
- Technology is progressing at a fast pace, therefore underspending or underinvesting may cause municipalities to fall behind with advancing their IT landscape.

The graph below shows the municipal IT OpEx for each peer municipality as a percentage of total municipal OpEx, in order from the smallest population on the left to the largest on the right

The peer group ranges from as low as 0.6% to as high as 2.8%, with an average of 1.8%.

- It is important to note these numbers are self-assessed and were provided to Blackline by each municipality as part of the peer study. There are some differences in the type of data sets – they are a mix of actuals, budgets or estimates. Additionally, the District provides support to two other municipalities and these expenses may be included in the provided operating expenses. If that's the case, then the District's percentage would be lower, lowering the peer average.

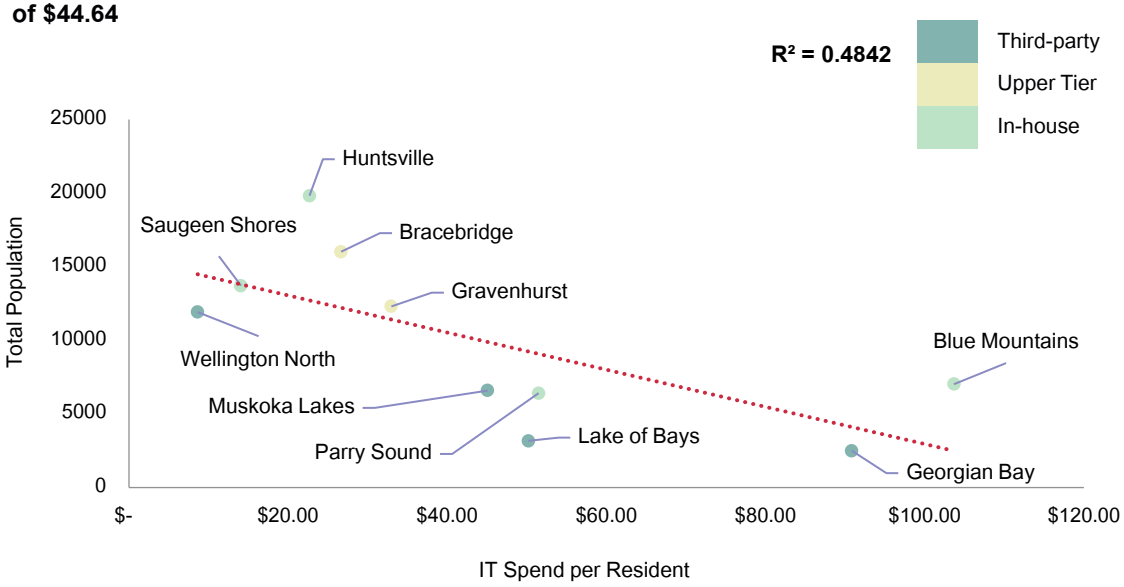


As population increases, IT spend per resident decreases

Insights

- The graph to the right shows that there is a moderate correlation between population and IT spend per resident. Peers with larger populations spend less on IT per resident than peers with smaller populations, likely due to some economies of scale.
- Peers that are below the trendline spend less per resident for their population. The graph shows that peers that outsource their IT services tend to fall below the trendline.
- This data would also suggest that these peers provide better value per resident. However, as we describe later in this report, the scope of IT services for third parties is smaller than that of in-house.

The IT spend per resident ranges from as low as $8.65 to as high as $103.70, with an average of $44.64



The majority of peers use more than one Internet Service Provider (ISP)

Insights

- There are five peers that have only one ISP. It is good practice to have more than one ISP. If the primary Internet connection fails, then the Internet traffic can be rerouted to the secondary.
- Fibre Internet connections typically have higher bandwidth and are more reliable. However, many of the peers are rural and have limited access to fibre, instead relying on wireless connections that can be greatly affected by weather. Some of the peers are part of regional projects to improve this:
  - Wellington North is participating through Wellington County in the Southwestern Integrated Fibre Technology (SWIFT) project. This is a non-profit municipally-led broadband expansion project created to improve Internet connectivity by laying fibre in rural areas across Southwestern Ontario.
  - The District of Muskoka has formed the Muskoka Economic Recovery Task Force, which is prioritizing getting broadband services for the whole region. However, this will be years before coming to fruition.
- A high-speed, reliable Internet connection is more important today than ever before.
  - Many of the peers discussed moving to Cloud-based municipal applications, which require a reliable connection so staff working from the office can access the Cloud-based software.
  - Some of the peers stated they will be shifting to a post-Covid hybrid work model, with some staff returning to the office while others continue to work from home. Without a reliable connection, remote staff will not be able to access on-site IT services.

We asked the peer group to provide the type and speed of all of their Internet connections, which we've summarized in the table below

Speed	
Lowest	40 Mbps
Highest	1 Gbps
Mode	100 Mbps
Type	
Fibre	Eight municipalities
Cable	One municipality
Wireless or Cellular	Five municipalities

- Five of the peers use more than one ISP. Given their proximity to each other, most of the peers use Lakeland and ViaNet as their ISPs.
- Many of the peers have rural areas within their municipalities. As such, those that are using fibre also need to use other connection types, as they are limited to where the fibre is located.
- Most peers have a 100 Mbps connection. Two have up to 1 Gbps speed.

All peers are concerned about ransomware attacks and seven have recently undergone a third-party cybersecurity review

Ransomware was noted by each peer as one of their top cybersecurity concerns

In addition to ransomware, four of the municipalities stated users are one of their main cyber risk concerns.

- Working from home has exacerbated this concern, as it is more difficult to ensure staff are following IT practices. For example, staff may be accessing their email from their home devices or may not be up to date on changes to their municipality's IT guidelines.
- Data loss, whether through malware or password theft, was also a common concern among peers. Those who stated this concern discussed their strategies of maintaining frequent back-ups to secondary sites or the Cloud.
- One of the municipalities expressed concerns about using Cloud applications. This is a concern often cited by other municipalities we've worked with as there is discomfort in not having full control of one's data security. However, many Cloud providers have rigorous security standards in place that can be more advanced than the municipality's due to the economies of scale that come with having multiple customers.

Seven peers have undergone a third-party cybersecurity review in the past three years

The peers differ in frequency of the reviews, with some conducting reviews every year and others on a two or three-year cycle. One municipality alternates each year between their corporate IT and their operational IT (e.g. SCADA systems). Below we describe the most common types of cybersecurity reviews and audits:

 **Penetration Test**	A hands-on examination by a real person that tries to detect and exploit weaknesses in your system. The goal is to simulate a hacker attempting to get into a business system, using methods such as password cracking or SQL injection.	Five of the peers state they have completed this
 **Vulnerability Assessment**	An automated, high-level scan of computers, systems and networks that looks for and reports potential security weaknesses known as vulnerabilities. These scans give an initial look at what could possibly be exploited.	None of the peers state they have completed this
 **Social Engineering**	A broad term used to describe a range of techniques to trick people into giving fraudsters sensitive information. This can occur on any platform or through any method, including even in-person visits, social media requests,	One of the peers state they have completed this
 **Phishing**	The most common under the social engineering umbrella, phishing is a specific technique designed to get users to share passwords, usually via email. The phishing message will appear legitimate to compel an employee to click on links and unwittingly give away sensitive information.	Five of the peers state they have completed this

Ontario municipalities are increasingly becoming targets for cyberattacks

Insights

In 2018, Wasaga Beach and Midland became targets with ransom demands; the full cost of recovery was estimated to be $250k. The Mayor of Stratford described Canadian municipalities as 'sitting ducks' for cyber terrorists after they suffered a ransomware attack and paid $75k in Bitcoin in 2019. For criminals, it is an easy opportunity to make money as they are aware that municipalities may not have the most sophisticated security measures. Often it may be cheaper to pay the ransom than put safeguards in place, thus local governments remain targets. To avoid being the next news headline, municipalities should build robust cybersecurity programs.

Security assessments are important as they identify vulnerabilities, expose potential threats, and identify strategies to safeguard IT infrastructure.

- Another important element is educating users on cybersecurity as many incidents occur unintendedly with staff. These can be simply avoided by ensuring staff are aware of how to respond in the event of a suspicious event.
- Typically, organizations that have sophisticated security systems and precautions also conduct regular reviews as cyberspace is rapidly evolving.
- At a minimum, municipal cybersecurity practices should include:
  - Ongoing phishing campaigns followed by education and training
  - Every two years, conduct a third-party vulnerability and penetration test
  - Maintain secure infrastructure with firewalls, anti-viruses, encrypted data, two-factor authentication, and backups to the Cloud

Cybersecurity practices varied among the peers; the following were common:

- Security-related infrastructure, including firewalls and network segmentation
- Multi-factor authentication
- Up-to-date anti-virus
- Encryption
- Patching strategy
- Continuous backups to secondary data sites and the Cloud
- Security policies that outline items such as password length, IT acceptable use, rights to file access
- Disaster recovery plans that include cyber response plans that are tested annually
- Ongoing training and education and phishing campaigns

Two of the peers expressed that they were unsure of what cybersecurity practices they had in place, as their third-party IT providers are responsible for this.

- In general, human ignorance is a major cybersecurity risk and we believe it is crucial for non-IT employees to understand what the municipality's cybersecurity practices are to ensure they adhere to them.

Peers with in-house IT functions funnel all IT-related decisions to their IT team for approval

Insights

- The diagram to the right is Blackline's model for IT governance. We believe that each of these groups should exist in some form for effective governance and decision-making. Each body does not need to exist independently, but it should just be clear who is making which decision.
- Where IT is outsourced, the municipality should have a designated staff member who has the responsibility of liaising with the third party.
- Commonly another role of IT leadership is facilitating partnership meetings where departments discuss their IT needs and establish corporate priorities. Among the peer group, five have IT committees that meet regularly and consist of representatives from IT and various departments.
- The Design Authority group decides on the specific technologies the municipality will use and the policies it will adopt – such as security.

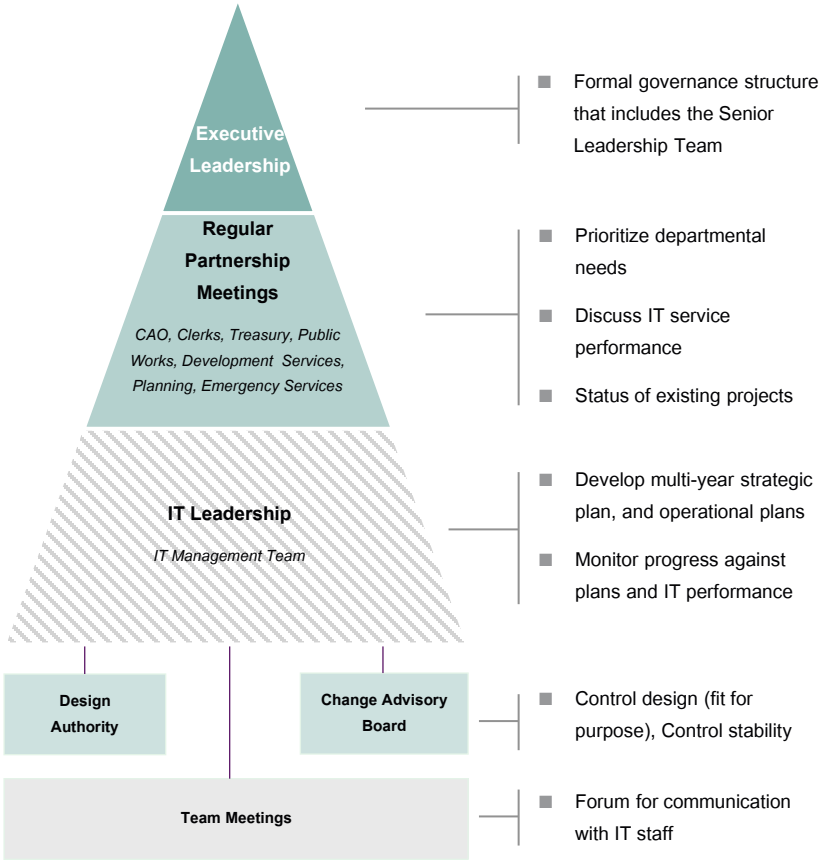
We asked each of the peers to describe their IT governance model and approach to decision-making

Of the six peers that outsource their IT, we saw two different decision-making structures, which we characterize as:

- Centralized – There is one person or group that reviews and approves all IT related-decisions and then seeks input from the third party, from buying software to updating policies and procedures. Three of the municipalities that outsource have this structure in place, two of which outsource to their upper tier.
- Decentralized – Each department within the municipality makes its own decisions related to technology. The departments may or may not go to the third party to get their input. Three of the municipalities that outsource have this structure in place.

For peers with internal IT staff, all IT-related decisions are reviewed and approved by the IT department, who ensure that the immediate and long-term needs of the municipality are taken into consideration so that IT decisions are prioritized appropriately.

IT Governance Model



Modernizing technology and improving security is a key priority for municipalities

When asked about the main priorities of each IT department over the next three years, there were some recurring themes among peers – security and modernization of technology were most occurring

Priority	Goal	Peer Feedback
Increasing Use of Cloud	To switch to Cloud-based applications to limit expensive hardware.	Two of the peers are focusing on increasing their use of Cloud over the coming years. One peer is in the process of migrating to a Cloud permitting solution, while the other has developed a cloud action plan that focuses on pushing application loads to the Cloud by way of vendors.
Improve Internet Connectivity	To improve current bandwidth and ensure minimal downtime.	Four of the peers discussed the need to improve their Internet connections. One of the peers has just built a new wireless tower that should improve connection speed 10-fold, while a few others are working either alone or in conjunction with neighbouring municipalities to bring fibre to their respective regions.
Modernize Technology	Modernize and procure new technology to ensure IT is up to date so that staff have the tools they need to be most efficient.	Eight of the peers stated that modernizing technology is one of their top priorities. For example, some of the peers will be procuring and implementing remote technologies such as tablets for their operational staff. One peer is migrating to TownSuites ERP, which has both a customer and employee portal, work order management and asset management capabilities. This will replace eight of their current systems, notably iCity, which is used by many in the peer group. Many of the peers will be increasing their online service functionality, including accepting credit card payments. Some peers are implementing document management solution to improve FOI searches.
Cybersecurity	Strengthen IT security to defend against cyber-attacks.	Five of the municipalities discussed their need to improve cybersecurity. Either they haven't undergone a review in the past three years, or they have but improving their cybersecurity practises is a priority. Specifically, these peers discussed procuring better firewalls, increasing the frequency of penetration tests, and implementing multi-factor authentication.
Microsoft Office 365	Deploy Office 365 tools to improve staff productivity.	While five of the peers have implemented Office 365, four are in the process and have made it one of their priorities over the next year. Two of the four have implemented Exchange Online and are now implementing the remaining office applications.

CYBERSECURITY POSITION

Cybersecurity is the measures used to secure an organization from malicious attacks via the Internet

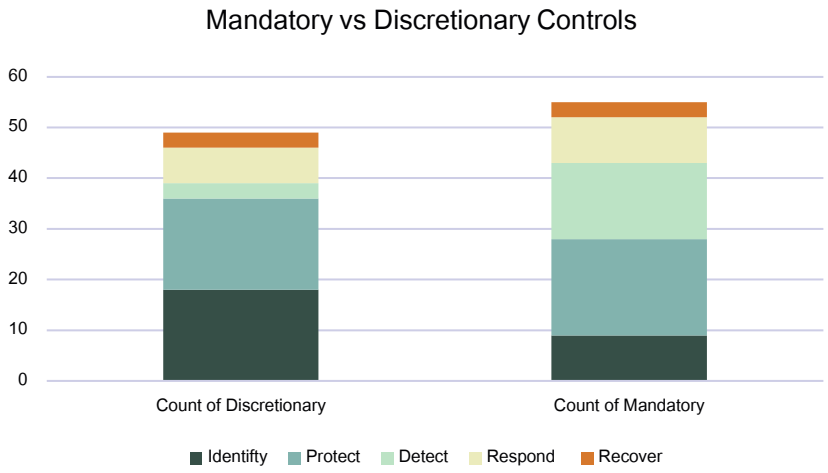
The National Institute of Standards and Technology (NIST) has developed a comprehensive framework for assessing an organization's cybersecurity

The framework considers measures to identify, protect, detect, respond and recover from cyber incidents.

- In each domain, NIST has identified a range of specific measures an organization should take to secure itself – 108 measures in total.
- However, not all of these measures necessarily apply to smaller organizations such as the Township. We have categorized the measures as either Mandatory – all organizations should apply these measures; or Discretionary – there are benefits, but the Township should only consider these after meeting all the mandatory measures.
- Additionally, some of the measures do not apply to the Township – for example, the Township does not operate critical infrastructure – so we removed those measures that are not applicable. Of the 108 measures, we excluded a total of 4 controls.

The chart to the lower right shows how the measures are distributed between the five domains.

- Identify and protect have the most measures and these can be considered the preventative domains.



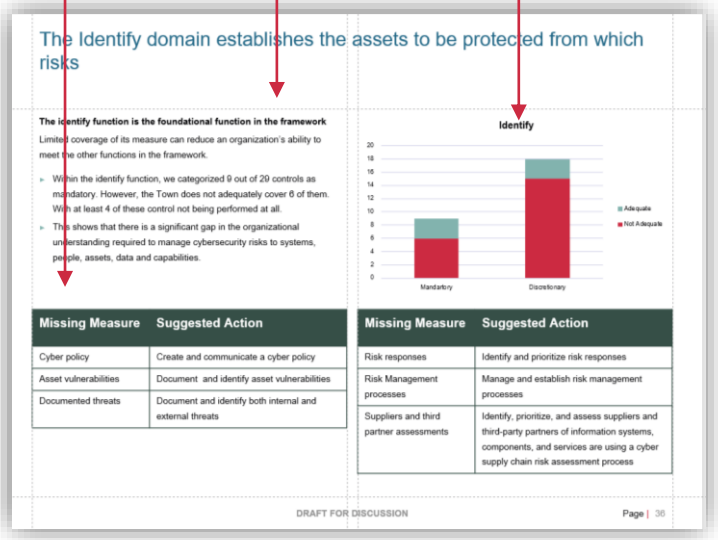
We used the NIST framework to assess the cybersecurity position of the Township

Through interviews and documentation review, we considered whether the Township has each of the cybersecurity measures in place or not

The measures in NIST are not prescriptive and clients can take many approaches to implementing any one of the measures.

- As such, as well as identifying the measure, we rated the effectiveness of how the Township had implemented the measure on a five-point scale. This list arranged from least effective to most:
  - N/A – measure not implemented
  - Partial – a measure has been implemented, but it does not cover the entire risk
  - Risk Informed – a measure has been implemented and is suitable to the risk faced by the organization
  - Repeatable – the measure is effective for the risk and is implemented in the same way each time it is applied
  - Adaptable – the measure is effective for the risk and is continuously improved as the environment evolves
- For this review, we are concerned primarily with mandatory controls that are rated N/A or partial. These have been categorized as “not adequate” while those rated, Risk Informed, Repeatable or Adaptable have been categorized as “adequate”.
- The graphic to the right shows how to read each of the following pages.

- Assessment – Blackline’s view of how well the Township has the domain implemented
- Scoring – the number of measures the Township’s has implemented adequately
- Actions – what we feel the Township should do to mitigate the missing measures

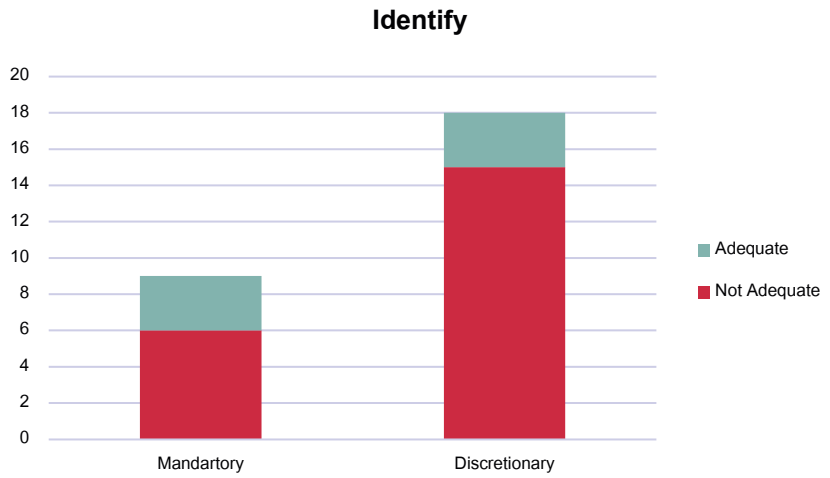


The Identify domain establishes the assets to be protected from which risks

The identify function is the foundational function in the framework

Limited coverage of its measure can reduce an organization's ability to meet the other functions in the framework.

- Within the identify function, we categorized 9 out of 29 controls as mandatory. However, the Township does not adequately cover 6 of them, with at least 4 of these control not being performed at all.
- This shows that there is a significant gap in the organizational understanding required to manage cybersecurity risks to systems, people, assets, data and capabilities.



Missing Measure	Suggested Action
Cyber policy	Create and communicate a cyber policy
Asset vulnerabilities	Document and identify asset vulnerabilities
Documented threats	Document and identify both internal and external threats

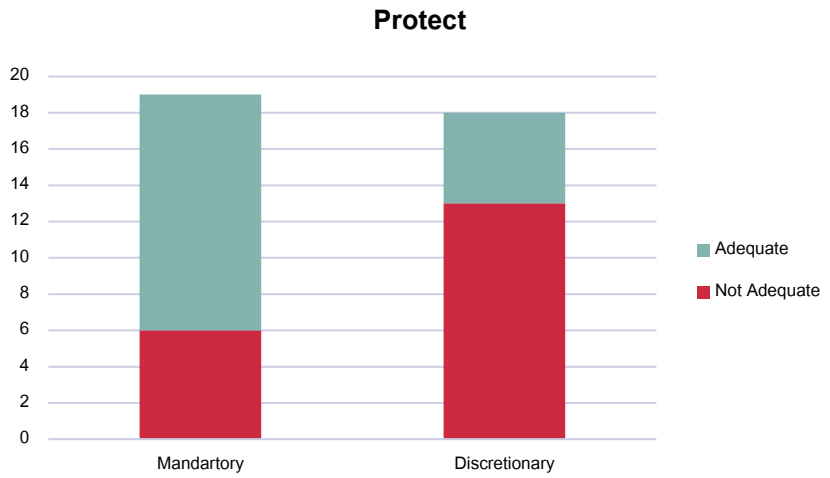
Missing Measure	Suggested Action
Risk responses	Identify and prioritize risk responses
Risk Management processes	Manage and establish risk management processes
Suppliers and third partner assessments	Identify, prioritize, and assess suppliers and third-party partners of information systems, components, and services are using a cyber supply chain risk assessment process

The Township makes considerable effort to ensure that its data is protected

The protect function is intended to develop and implement appropriate safeguards to prevent malicious incidents

This is commonly the first area an organization will think about when considering IT security generally.

- Within the protect function, we categorize 19 of the 39 controls as mandatory. The Township has about eight repeatable measures in place, however, four measures are not implemented.
- While the Township does make a good effort to protect its data, only some members of senior management are aware of their roles and responsibilities in protecting it.



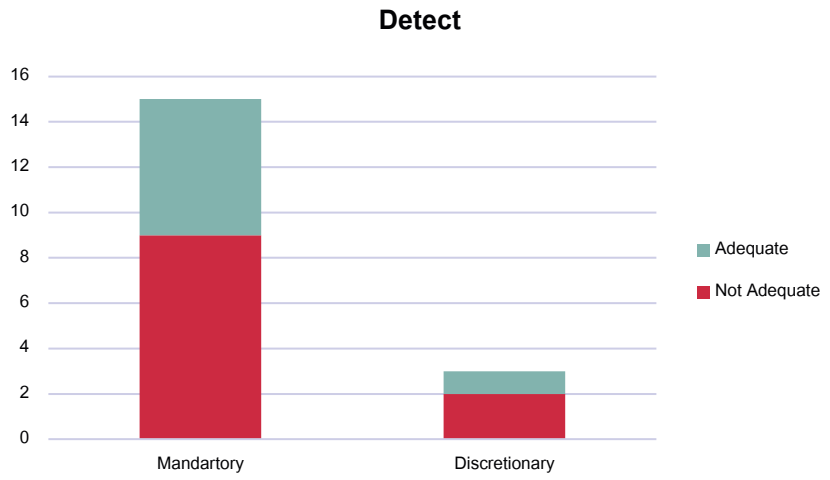
Missing Measure	Suggested Action
Cyber roles and responsibilities	Ensure physical and cybersecurity personnel understand their roles and responsibilities
Data leak protection	Protections against data leaks are implemented
Response and recovery plan testing	Ensure response and recovery plans are tested regularly

Missing Measure	Suggested Action
Communications and control networks protection	Ensure communications and control networks are protected
Formal access permissions	Formally document, manage and enforce access permissions and incorporating the principles of least privilege and separation of duties
Training	Establish formal mandatory training for all users

The detect domain indicates how effective an organization will be in noticing an incident is occurring

83% (15 out of 18) of the controls in the detect function are mandatory

- The detect function is the equivalent of installing smoke alarms in a home. This function emphasizes the development and implementation of activities that identify the occurrence of a cyber event in a timely manner. Timeliness is important because it is directly correlated with increased impact - the longer an attack continues increases the likelihood of data loss or other damages.
- Amongst the 15 mandatory controls in the detect function, the Township did not show evidence or documentation for six of them. For instance, the Township does not monitor its external service provider activity for potential cyber events.



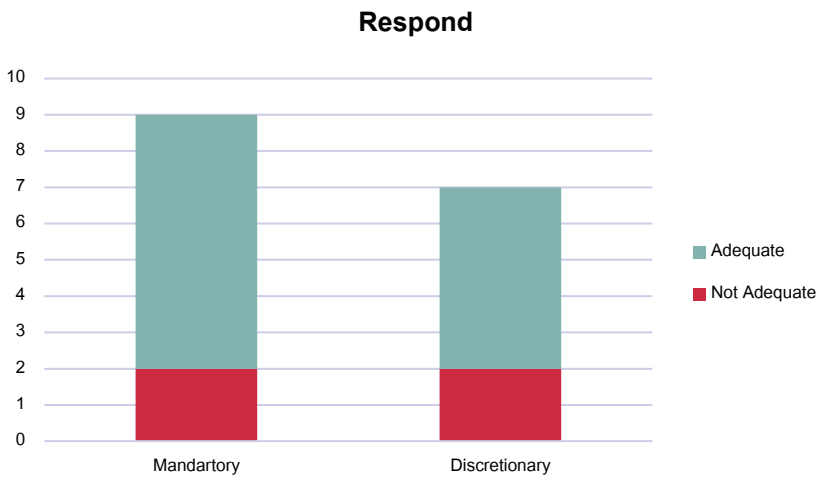
Missing Measure	Suggested Action
Network operations and data flows	Establish and mange a baseline of network operations and expected data flows for users and systems
Incident alerts	Establish incident alert thresholds
Personnel activity	Monitor personnel activity to detect potential cybersecurity events
Third party provider monitoring	Monitor external service provider activity to detect potential cybersecurity events

Missing Measure	Suggested Action
Monitoring of physical environment	Ensure the physical environment is monitored to detect potential cybersecurity events
Detection of roles and responsibilities	Define roles and responsibilities for detection to ensure accountability
Test detection processes	Perform penetration test
Improve detection processes	Perform penetration test
Vulnerability scan	Perform vulnerability scans

Respond is where the Township has the most coverage

9 out of 16 of the controls in the respond function are mandatory

- The respond function includes appropriate activities to undertake during a detected cyber event. It focuses on the organization's ability to contain the impact of a cyber event.
- Although the Township has never had a cyber event, it, at least partially, showed evidence and documentation for seven of the nine mandatory measures.

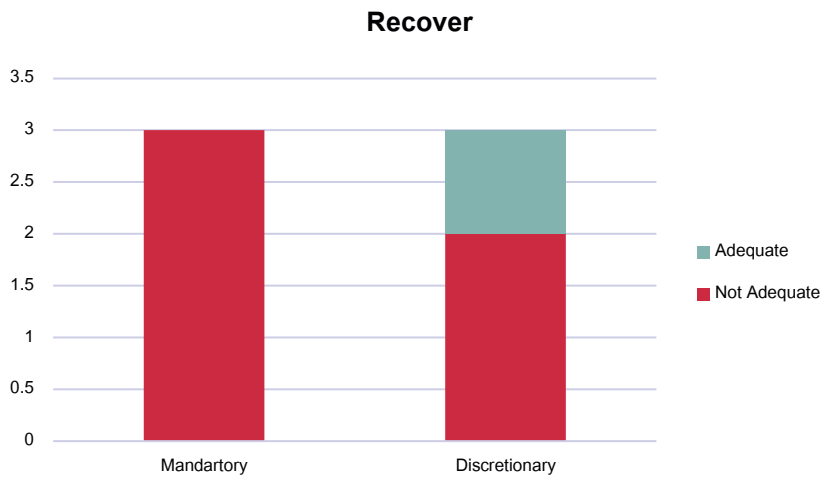


Missing Measure	Suggested Action
Impact analysis	Perform impact analysis following an incident to ensure the impact of the incident is understood
Forensics	Ensure forensics are performed after an incident

The Township did not show evidence of a recovery plan

Half of the controls (3 out of 6) in the recover function are mandatory

- The recover function identifies appropriate activities to maintain plans for resilience and to restore capabilities or services that have been impaired due to a cyber security incident. It emphasizes and supports a timely return to normal operations to reduce the impact of a cybersecurity event.
- These three mandatory controls not adequately performed in the recover tab are related to the creation of a recovery plan. The first control requires the Township to develop a recovery plan. The Township began this process at the onset of the COVID-19 pandemic but is yet to complete it. As a result, it is not able to perform the other two functions: incorporation of recovery plans and updating of recovery strategies.

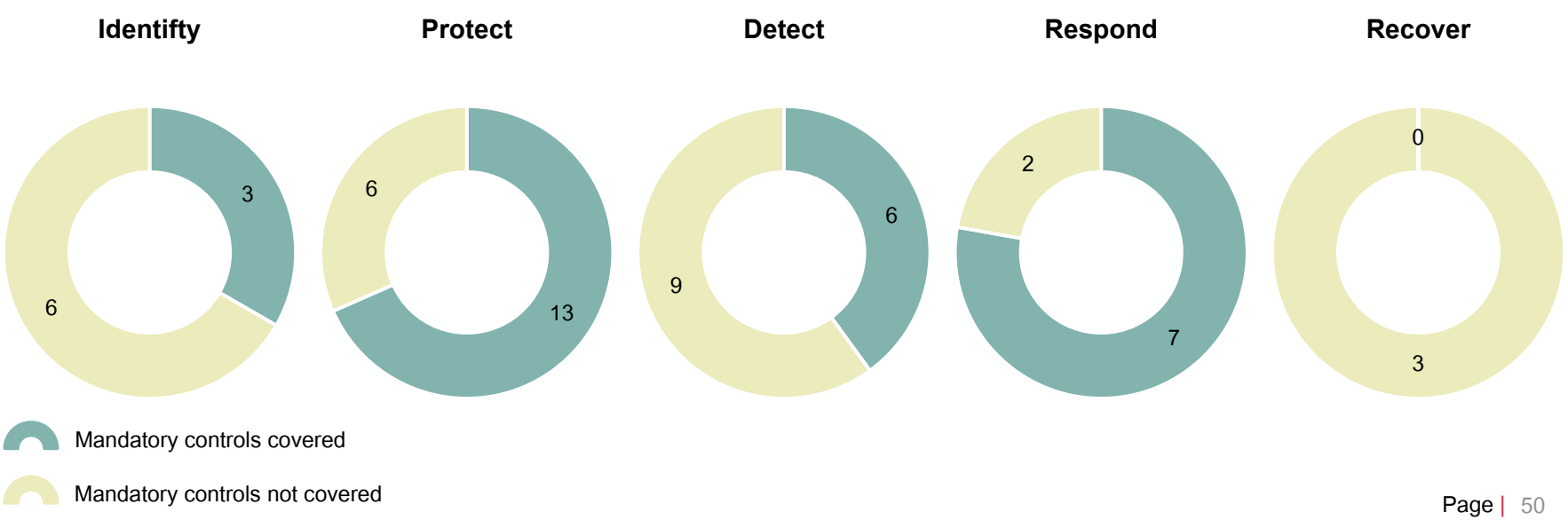


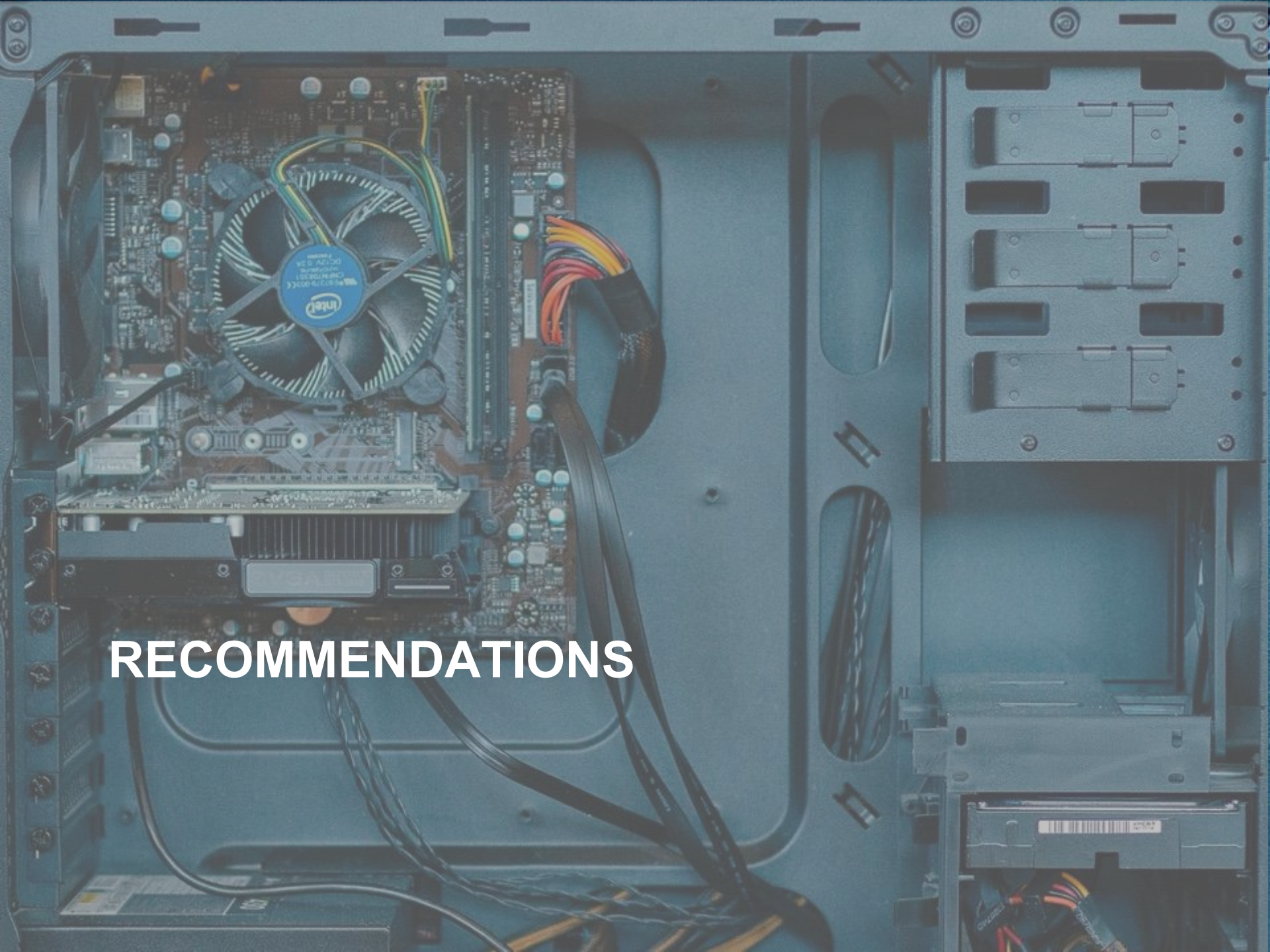
Missing Measure	Suggested Action
Execute recovery plan during cyber event	Complete recovery plan
Incorporate lessons learned in recovery plans	Complete recovery plan
Update recovery plan strategies	Complete recovery plan

Muskoka Lakes should prioritize developing its plan in the event of a cyber incident

The chart at the foot of the page shows the comparison of the five domains and the coverage the Township has of the mandatory measures in each domain

- Potentially the biggest gap is a response and recovery plan. This plan would outline the various sorts of incidents the Township might face, how it would respond once it detected the incident and how it would recover if systems were compromised.
- Ransomware is one of the greatest concerns among municipalities, with most of the peers we spoke to indicating it was what they were most concerned about. A response and recovery plan for this scenario might include details on situations where the Township would and would not pay the ransom.





RECOMMENDATIONS

The current Strategic Plan has implications for IT

The Township has set four strategic goals

Within the third goal, Enhance and Sustain Public Services and Infrastructure, it states:

"Assess the Township's current service delivery models and identify opportunities for modernization, digitization, and enhanced customer service engagement."

- This obviously speaks to information technology directly. As we have developed the recommendations in this report, we have used this as a directional statement.

Using the strategic plan direction, input from staff and our assessment of the current state, we have created a set of recommendations for the Township.

- We have grouped our recommendations under three pillars that explain the objective of this IT strategic plan

Over the following pages, we elaborate on these recommendations and highlight their ongoing financial impact

		#	Recommendation
Reinvent the Resident Experience	Recent experience has emphasized the benefits of offering services digitally and online. To expand the online offering the Township will need to enhance the capabilities of the existing website, ideally, creating a portal that residents can log into to access Township services and see a history of their interactions.	1.	Create portal
		2.	Migrate services
		3.	Add payment capabilities
		4.	Market to residents
		5.	Connect to operational systems
Automate Business Processes	A number of the current systems do not meet the needs of the Township and should be replace. Additionally, there are process that do not have good system support that would benefit from automation and technology.	6.	Finish current projects
		7.	Migrate to Office 365
		8.	Replace the finance system
		9.	Establish workflow, approvals and digital signatures
		10.	Implement an HR solution
		11.	Eliminate paper time recording
Upgrade the IT Capabilities	After you establish your next managed services agreement, work with the provider to upgrade aspects of the IT infrastructure to enable more advanced capabilities.	12.	Fibre broadband Internet connection
		13.	Review site connection speeds
		14.	Review the phone systems
		15.	Investigate mobile technologies for staff that are mobile

Reinvent the resident experience

Situation

The current website is largely informational, with a number of PDF forms residents can download and complete. Muskoka does of the tax portal where residents can view information and pay a tax bill.

Recommendation

Deliver a range of Township services online, including the ability to make payments for fees and penalties.

Dependencies

Since the website is hosted outside of the Township, upgrades to the infrastructure are not required.

- Internet connectivity: that said, communication between the website and operational system will require a more reliable Internet connection.

Benefits

- Residents can access services in a more convenient and efficient manner.
- Cost to deliver services may go down as the online costs less than in-person services.

Risks

- Greater security risk keeping resident information online.

#	Initiative	Financial Impact	Change
1	**Create portal** Enhance website with the capabilities to register and sign in users to a private, secure area where they can access their information and Township Services.	Software: ↑ Hardware: —	Medium
2	**Migrate services** In a phased manner, make services available within the portal. This will require online forms, bookings, workflows and other capabilities depending on the service.	Software: — Hardware: —	None
3	**Add payment capabilities** A general online payment gateway along with the ability to calculate payments required.	Software: ↑ Hardware: —	Low
4	**Market to residents** Make residents aware of the new options and promote their use over in-person.	Software: — Hardware: —	None
5	**Connect to operational systems** The transaction completed online will require staff to act in some cases. To do this, information must flow from the online service to the operational system that staff use	Software: ↑ Hardware: —	Medium

Automate business processes

Situation

The Township has a range of systems that support some, but not all, its processes. In some cases, these systems do not meet the Townships needs.

Recommendation

Invest in automating many of the manual processes that occupy staff time and replace systems that are not fit for purpose. Investigate other processes that could be automated.

Dependencies

- Internet connectivity: many of the solutions, particularly Office 365, are Cloud-based and will require good connectivity.

Benefits

- Frees staff time to focus on more important aspects of service delivery.

Risks

- Creates a more complex IT environment, where systems are required to deliver services.

#	Initiative	Financial Impact	Change
6	**Finish current projects** The Township is implementing a record management system and a work order system, both projects should be completed.	Software: ↑ Hardware: —	Low
7	**Migrate to Microsoft Office 365** The current Office product offers a range of benefits over the on-premise approach the Township is taking.	Software: ↓ Hardware: ↓	Medium
8	**Replace the finance system** The current system does not meet the Township's needs and is not being kept current by the vendor.	Software: ↑ Hardware: —	Medium
9	**Establish workflow, approvals and digital signatures** To operate more digitally means the Township needs to replace the flow of paper that enables many processes with electronic workflows. Additionally, both in policy and technology, establish an accepted digital signature.	Software: ↑ Hardware: ↑	Medium
10	**Implement an HR solution** Employee records and information should be kept electronically for security, ease of access and efficiency.	Software: ↑ Hardware: —	Low
11	**Eliminate paper time recording** Paper timesheets lead to much rekeying in order to drive the payroll process.	Software: ↑ Hardware: ↑	Medium

Upgrade the IT capabilities

Situation

The IT infrastructure at the Township is generally suitable, but as the Township delivers more services online, automates more processes and moves systems to the Cloud, some changes will be required.

Recommendation

Upgrade the communications infrastructure to fully support the new work model that technology offers.

Dependencies

- Availability: with networking, the Township is somewhat reliant on what local telecoms providers plan to implement by way of fibre.
- In parallel: not strictly a dependency, but we recommend the infrastructure is enhanced along with the other changes, not in preparation for the other changes.

Benefits

- Frees staff time to focus on more important aspects of service delivery.

Risks

- None beyond standard implementation risks.

#	Initiative	Financial Impact	Change
12	**Fibre broadband Internet connection** Explore ways to get fibre connections for Township offices in order to increase the bandwidth and increase the reliability of Internet connectivity.	Software: — Hardware: ↑	Low
13	**Review site connection speeds** Depending on the technology used, and planned to be used, at each site, the existing inter-site connections may not be adequate.	Software: — Hardware: ↑	Low
14	**Review the communication systems** With a hybrid work model likely to continue, the Township should have a phone system that enables that way of working. On top of phones, video conferencing and online chat are features that have proven very effective.	Software: — Hardware: ↑	Low
15	**Investigate mobile technologies for staff that are mobile** For staff who are not office-based, being more digital in an efficient way will require mobile technologies. Examples include for building inspectors to complete inspection reports on-site, for road crews to look up and complete work orders and record time.	Software: ↑ Hardware: ↑	Low

Resource for success

Certain activities related to operating IT will always be the responsibility of the Township

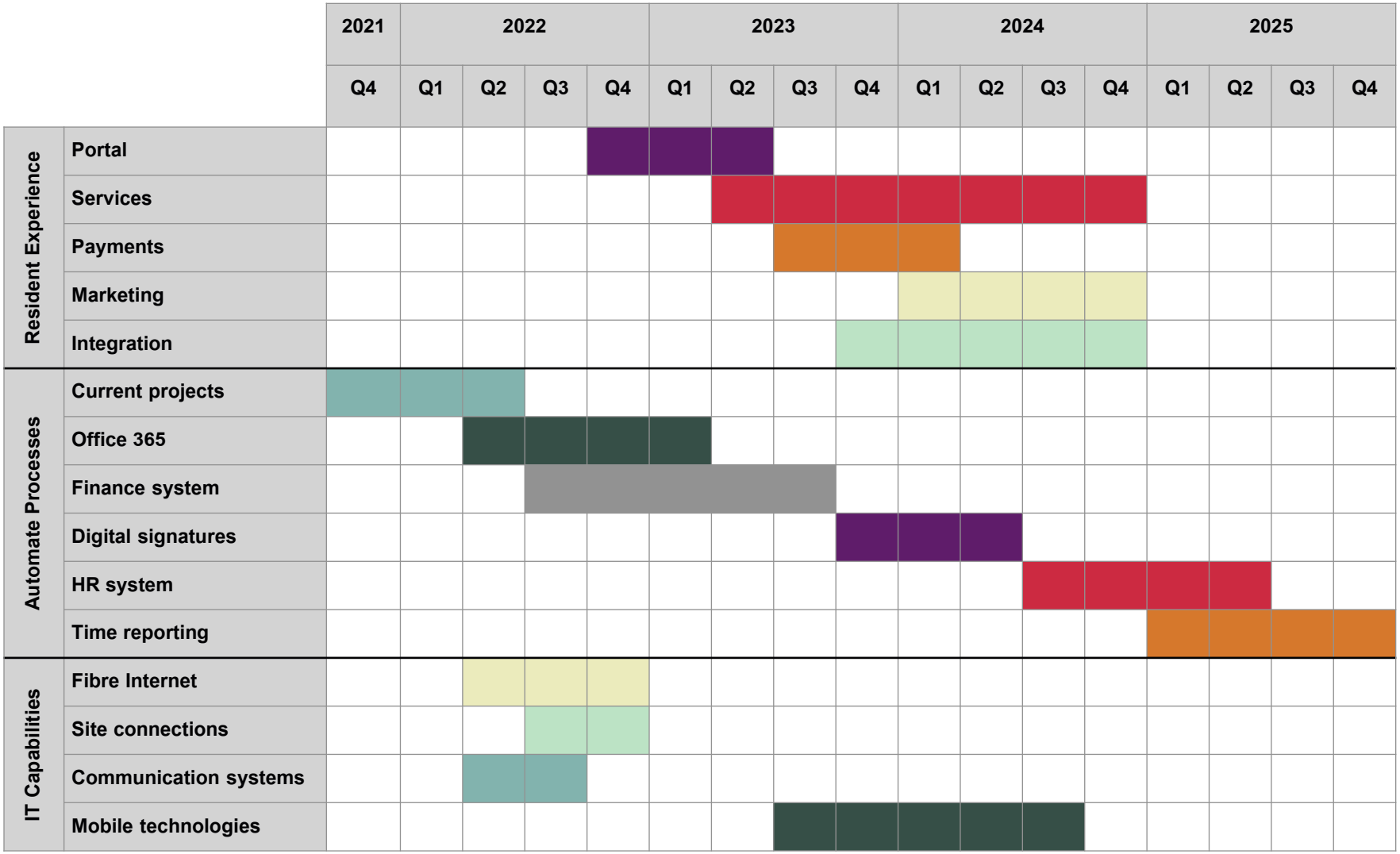
As such, the Township should hire a person who can provide you with project coordination, strategic direction, vendor coordination, governance and other IT activities.

- The table below shows our suggested work plan for the IT resource for the first 18 months.

Establish internal governance	Review the needs of the organization	Create a disaster recovery plan	Document the existing systems	Take administrative responsibility	Create cyber-response plan
Define how decisions about IT are made and who gets to make them	Working with departmental staff, complete a full review of processes and IT needs to augment this strategy	The plan should allow the Township's IT to continue to operate under a variety of scenarios	Create documents and diagrams showing the network and server infrastructure	Ensure the Township has administrator access to all systems and that vendors use unique accounts	The set of instructions the Township will follow to prepare for, detect, respond to, and recover from network security incidents.

Additionally, GIS should be a critical system to the Township, but ready access to a technical resources that can configure GIS and update the information contained within should be put in place

We have sequenced the recommendations over a four-year period



APPENDICES

Appendix A
Application Index

#	Application Name	Vendor	Department
1	iCity	CentralSquare	Finance/payroll
2	Questica Budgeting	Questica	Finance
3	CityWorks	ESRI	Public Works
4	FirePro		Fire Services
5	Shopkey Pro (Snapon)	Mitchell 1	Public Works (Garage)
6	Insite	Cummins	Public Works (Garage)
7	Allison Transmission Software	Noregon	Public Works (Garage)
8	CatET	Caterpillar	Public Works (Garage)
9	Diagnostic Link		Public Works (Garage)
10	Laserfiche	ThinkDox	Clerk
11	M-Files (in progress)		Clerk
12	HRWize	Diabsolut	HR/Payroll
13	JASI		Library
14	CivicWeb	iCompass	Clerks
15	Stone Orchard	CentralSquare	Public Works (Cemetery)
16	HootSuite		Social Media Management

#	Application Name	Vendor	Department
17	Land Information System Application	Marmak	Building
18	Facebook		Communications
19	Constant Contact		Communications
20	Canva		Communications
21	BangTheTable		Communications
22	GIS	ESRI	Public Works
23	MAM		Public Works (Payroll)
24	BookKing		Recreation
25	SafetyNow	Bongarde	
26	CanNet	Cansel	Public Works
27	FluentIMS	Fluent	Fire Services
28	MapInfo Pro	PitneyBowes	Public Works
29	Quickbooks	Quickbooks	
30	TSCareer	MedTeq	HR
31	Winfuel		Public Works
32	WoodWorks Sizer	Canadian Wood Council	Building

Appendix B
Peer Questionnaire

Q1	What is the total number of municipal staff?
Q2	Do you have an internal IT department? If so, how many staff does your IT Department have? What is the split between full-time, part-time, and occasional?
Q3	Do you use any 3rd parties or contractors to help support IT services, for example, for helpdesk, application support, infrastructure refresh projects, etc. Can you please describe what is managed in-house versus outsourced and why you chose this balance?
Q4	Are there any key issues and challenges the IT Department is currently working upon?
Q5	What are the priorities the IT Department is focusing on for the next 3 year? What specific innovative technologies are you interested in pursuing?
Q6	What was your 2019 IT OpEx and IT CapEx? And what was your total 2019 municipal OpEx and CapEx? Were your IT expense in 2020 affected by COVID?
Q7	Please describe the IT governance structure and how decisions about IT priorities and implementing new systems are made.
Q8	Have you had a 3rd party cybersecurity review in the past 3 years? What cybersecurity practices do you have in place? Are you considering changing any practices or adding new ones in the near future?
Q9	What are the main cyber risks you are concerned about?
Q10	Are you using or plan to use MS Office 365? If so, will you use the on-premise or Cloud option?
Q11	Can you please provide us with: - Speed of connection - Type of connection
Q12	What are the key municipal systems you use (e.g. your finance system, public works/asset management systems)? What are the strengths and weaknesses behind these systems and why did you choose them?

Appendix C
NIST cyber framework and Township effectiveness - Identify

Category	Subcategory	Criticality	Effectiveness
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	Mandatory	2 - Risk Informed
	ID.AM-2: Software platforms and applications within the organization are inventoried	Discretionary	0 - N/A
	ID.AM-3: Organizational communication and data flows are mapped	Discretionary	0 - N/A
	ID.AM-4: External information systems are catalogued	Discretionary	0 - N/A
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Discretionary	0 - N/A
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Mandatory	2 - Risk Informed
Business Environment	ID.BE-1: The organization's role in the supply chain is identified and communicated	Discretionary	3 - Repeatable
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Not Applicable	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Discretionary	3 - Repeatable
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Discretionary	1 - Partial
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Discretionary	1 - Partial

Appendix C

NIST cyber framework and Township effectiveness - Identify

Category	Subcategory	Criticality	Effectiveness
Governance	ID.GV-1: Organizational cybersecurity policy is established and communicated	Mandatory	1 - Partial
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Discretionary	1 - Partial
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Discretionary	0 - N/A
	ID.GV-4: Governance and risk management processes address cybersecurity risks	Mandatory	2 - Risk Informed
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	Mandatory	0 - N/A
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Discretionary	0 - N/A
	ID.RA-3: Threats, both internal and external, are identified and documented	Mandatory	1 - Partial
	ID.RA-4: Potential business impacts and likelihoods are identified	Discretionary	0 - N/A
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Discretionary	0 - N/A
	ID.RA-6: Risk responses are identified and prioritized	Mandatory	0 - N/A
Risk Management Strategy	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Mandatory	0 - N/A
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Discretionary	0 - N/A
	ID.RM-3: The organization determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Not Applicable	

Appendix C

NIST cyber framework and Township effectiveness - Identify

Category	Subcategory	Criticality	Effectiveness
Supply Chain Risk	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Discretionary	0 - N/A
Management	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Mandatory	0 - N/A
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Discretionary	0 - N/A
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Discretionary	0 - N/A
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Discretionary	2 - Risk Informed

Appendix C

NIST cyber framework and Township effectiveness - Protect

Category	Subcategory	Criticality	Effectiveness
Identity Management, Authentication and Access Control	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Mandatory	3 - Repeatable
	PR.AC-2: Physical access to assets is managed and protected	Mandatory	2 - Risk Informed
	PR.AC-3: Remote access is managed	Mandatory	3 - Repeatable
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Mandatory	1 - Partial
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Mandatory	2 - Risk Informed
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Discretionary	3 - Repeatable
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individual's security and privacy risks and other organizational risks)	Mandatory	3 - Repeatable
Awareness and Training	PR.AT-1: All users are informed and trained	Mandatory	1 - Partial
	PR.AT-2: Privileged users understand their roles and responsibilities	Mandatory	3 - Repeatable

Appendix C
NIST cyber framework and Township effectiveness - Protect

Category	Subcategory	Criticality	Effectiveness
Awareness and Training	PR.AT-3: Third-party stakeholders (e.g. Suppliers, customers, partners) understand their roles and responsibilities	Discretionary	1 - Partial
	PR.AT-4: Senior executives understand their roles and responsibilities	Discretionary	1 - Partial
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	Mandatory	0 - N/A
Data Security	PR.DS-1: Data-at-rest is protected	Mandatory	3 - Repeatable
	PR.DS-2: Data-in-transit is protected	Mandatory	2 - Risk Informed
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Discretionary	0 - N/A
	PR.DS-4: Adequate capacity to ensure availability is maintained	Discretionary	0 - N/A
	PR.DS-5: Protections against data leaks are implemented	Mandatory	0 - N/A
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Mandatory	3 - Repeatable
	PR.DS-7: The development and testing environment(s) are separate from the production environment	Not Applicable	
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Discretionary	0 - N/A

Appendix C

NIST cyber framework and Township effectiveness - Protect

Category	Subcategory	Criticality	Effectiveness
Information Protection	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Not Applicable	
Processes and Procedures	PR.IP-2: A System Development Life Cycle to manage systems is implemented	Discretionary	1 - Partial
	PR.IP-3: Configuration change control processes are in place	Discretionary	0 - N/A
	PR.IP-4: Backups of information are conducted, maintained, and tested	Mandatory	2 - Risk Informed
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Mandatory	3 - Repeatable
	PR.IP-6: Data is destroyed according to policy	Mandatory	2 - Risk Informed
	PR.IP-7: Protection processes are improved	Discretionary	2 - Risk Informed
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	Discretionary	1 - Partial
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Mandatory	3 - Repeatable

Appendix C
NIST cyber framework and Township effectiveness - Protect

Category	Subcategory	Criticality	Effectiveness
Processes and Procedures	PR.IP-10: Response and recovery plans are tested	Mandatory	0 - N/A
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Discretionary	3 - Repeatable
	PR.IP-12: A vulnerability management plan is developed and implemented	Discretionary	0 - N/A
Maintenance	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Discretionary	3 - Repeatable
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Discretionary	2 - Risk Informed
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Discretionary	1 - Partial
	PR.PT-2: Removable media is protected and its use restricted according to policy	Discretionary	0 - N/A
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Discretionary	0 - N/A
	PR.PT-4: Communications and control networks are protected	Mandatory	0 - N/A
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Discretionary	1 - Partial

Appendix C
NIST cyber framework and Township effectiveness - Detect

Category	Subcategory	Criticality	Effectiveness
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Mandatory	0 - N/A
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	Mandatory	2 - Risk Informed
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Discretionary	0 - N/A
	DE.AE-4: Impact of events is determined	Mandatory	2 - Risk Informed
	DE.AE-5: Incident alert thresholds are established	Mandatory	0 - N/A
Security Continuous	DE.CM-1: The network is monitored to detect potential cybersecurity events	Mandatory	3 - Repeatable
Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Mandatory	1 - Partial
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Mandatory	0 - N/A
	DE.CM-4: Malicious code is detected	Mandatory	2 - Risk Informed
	DE.CM-5: Unauthorized mobile code is detected	Discretionary	2 - Risk Informed
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Mandatory	0 - N/A
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Mandatory	2 - Risk Informed
	DE.CM-8: Vulnerability scans are performed	Mandatory	1 - Partial

Appendix C

NIST cyber framework and Township effectiveness - Detect

Category	Subcategory	Criticality	Effectiveness
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Mandatory	1 - Partial
	DE.DP-2: Detection activities comply with all applicable requirements	Discretionary	0 - N/A
	DE.DP-3: Detection processes are tested	Mandatory	0 - N/A
	DE.DP-4: Event detection information is communicated	Mandatory	2 - Risk Informed
	DE.DP-5: Detection processes are continuously improved	Mandatory	0 - N/A

Appendix C
NIST cyber framework and Township effectiveness - Respond

Category	Subcategory	Criticality	Effectiveness
Response Planning	RS.RP-1: Response plan is executed during or after an incident	Mandatory	3 - Repeatable
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	Discretionary	4 - Adaptable
	RS.CO-2: Incidents are reported consistent with established criteria	Discretionary	2 - Risk Informed
	RS.CO-3: Information is shared consistent with response plans	Discretionary	4 - Adaptable
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Discretionary	3 - Repeatable
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Discretionary	3 - Repeatable
Analysis	RS.AN-1: Notifications from detection systems are investigated	Mandatory	3 - Repeatable
	RS.AN-2: The impact of the incident is understood	Mandatory	1 - Partial
	RS.AN-3: Forensics are performed	Mandatory	1 - Partial
	RS.AN-4: Incidents are categorized consistent with response plans	Discretionary	3 - Repeatable
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Discretionary	2 - Risk Informed

Appendix C

NIST cyber framework and Township effectiveness - Respond

Category	Subcategory	Criticality	Effectiveness
Mitigation	RS.MI-1: Incidents are contained	Mandatory	3 - Repeatable
	RS.MI-2: Incidents are mitigated	Mandatory	3 - Repeatable
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Mandatory	3 - Repeatable
Improvements	RS.IM-1: Response plans incorporate lessons learned	Mandatory	3 - Repeatable
	RS.IM-2: Response strategies are updated	Mandatory	3 - Repeatable

Appendix C

NIST cyber framework and Township effectiveness - Recover

Category	Subcategory	Criticality	Effectiveness
Recovery Planning	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	Mandatory	1 - Partial
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	Mandatory	0 - N/A
	RC.IM-2: Recovery strategies are updated	Mandatory	0 - N/A
Communications	RC.CO-1: Public relations are managed	Discretionary	1 - Partial
	RC.CO-2: Reputation is repaired after an incident	Discretionary	1 - Partial
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Discretionary	2 - Risk Informed