BLACKLINE CONSULTING

A Higher Standard

IT Services Delivery Review

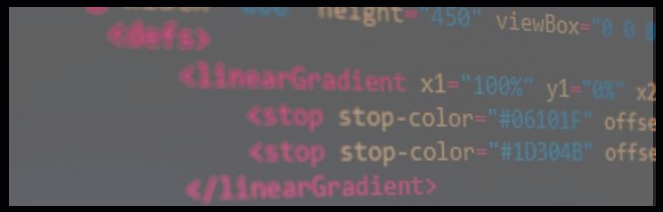
Final Report

The Corporation of the County of Wellington and Member Municipalities

November 2020

Private and Confidential

CONTENTS



/ CONTEXT – 3

/ EXECUTIVE SUMMARY – 6

/ RECOMMENDATIONS – 14

/ APPENDIX – 54

The purpose of this engagement is to review the current IT environments and identify opportunities for increased efficiency

Background

In 2019, The County of Wellington ("the County") and its seven member municipalities participated in an Operational Service Efficiency Review in response to the Government of Ontario's Provincial Modernization Grant. The review included (among others) an opportunity to "Explore common IT systems and resources across the County and local municipalities".[1]

Consequently, the County issued a Request for Proposal - Project Number CW2020-006 ("the Review") in February 2020. The objective of this engagement is to identify opportunities to reduce costs or improve efficiencies from achieving economies of scale.

Blackline Consulting ("Blackline") was selected to conduct the Review. The project began in late March 2020, however, due to COVID-19 the project experienced delays. Fieldwork and data collection occurred between May and August 2020. As such, data presented in this report is at a point in time, changes to data, such as the number of various IT equipment may have occurred during the publishing of this report.

As per the Ministry of Municipal Affairs and Housing requirements:

- The County acknowledges support by the Province for the project.
- The views expressed in this report are the those of Blackline and do not necessarily reflect those of the Province.

Our Scope

The scope of the Review includes the following municipalities:

- The County
- Township of Centre Wellington
- Township of Guelph/Eramosa
- Township of Mapleton
- Town of Minto
- Town of Wellington North
- Township of Puslinch

From a technical perspective the scope of the Review includes:

Review managed service agreements with third parties

Review existing hardware / software stacks

Review network architecture to increase stability

Identify potential to leverage cloud computing

The following page provides an overview of our approach.

1. County and Member Municipalities Complete Operational Service Efficiency Review

We tailored our approach to meet the Review requirements

Approach

Blackline has a standard methodology for conducting IT service deliver reviews. We tailored our approach to meet the specific requirements as describe in the RFP. Below we provide an outline of our approach for this Review:

Phase One – Discovery

During this phase we gathered documents and conducted interviews to get a perspective of the IT operations.

Phase Two – Analysis

Using the documentation and perspectives gathered in phase one, we reviewed the third-party service agreements, existing hardware and software, network stability and cloud computing.

Phase Three – Insight

In this phase, we identified alternative solutions. We took more than one approach in order to evaluate each potential opportunity properly.

Phase Four – Reporting

We formally documented the recommendations into this final report.

In This Document

This document is a culmination of our analysis.

- We created IT profiles for each member municipality. Within the profiles we summarize the IT environment across five key categories 1) IT financials, 2) service delivery, 3) software, 4) hardware and 5) network stability, and document our observations.
- From our observations we identified nine recommendations to improve the current IT environment. In this document, we present each recommendation as a mini business case which includes a) description of the situation b) the recommendation, c) a detailed step-by-step action plan, d) the benefits, and e) the financial impact and assumptions.

Glossary of Terms

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

/ EXECUTIVE SUMMARY

There are many disparities across the participating municipalities

Two of the municipalities have in-house IT resources

The remaining five use third parties to deliver a similar scope of IT services

- However, the contractual terms vary greatly among these five, with contract costs ranging from $25k to $43k, annually.
- There are many deficiencies in the contract terms, including:
  - Limited descriptions of scope of service, which may lead to unclear accountability between the customer and vendor
  - Undefined SLAs, which can lead to a mismatch of expectations
  - Unclear impact of volume on cost

There is a high variance of total IT spend per municipal staff

While the group average is $3,530 per municipal staff, the range is from $1,368 to $5,971.*

- This is reflective of the different IT environments, including the number of applications and the sophistication of the municipality's network and hardware resiliency.

The municipalities assess Cloud on a case-by-case basis in the absence of a formal framework

All have an appetite for Cloud and recognize Cloud is becoming the choice for vendors which will require municipalities to adopt.

There are several systems that are used by more than one municipality

Examples include Keystone and EasyPay Payroll, which are due for replacements for some of the municipalities, providing an opportunity to collaborate.

- Conversely, only two of the seven municipalities are using MS Office 365 on the Cloud. The remaining use on-premise versions, limiting the ability to benefit from collaboration and remote work functionality.

Hardware brands vary across the municipalities

However, products from HP, Dell and Lenovo are the most common end user equipment.

- Municipalities also differ in their refresh cycles and their adherence.

* Based on three year average (2017-2019) for both operating and capital expenses.

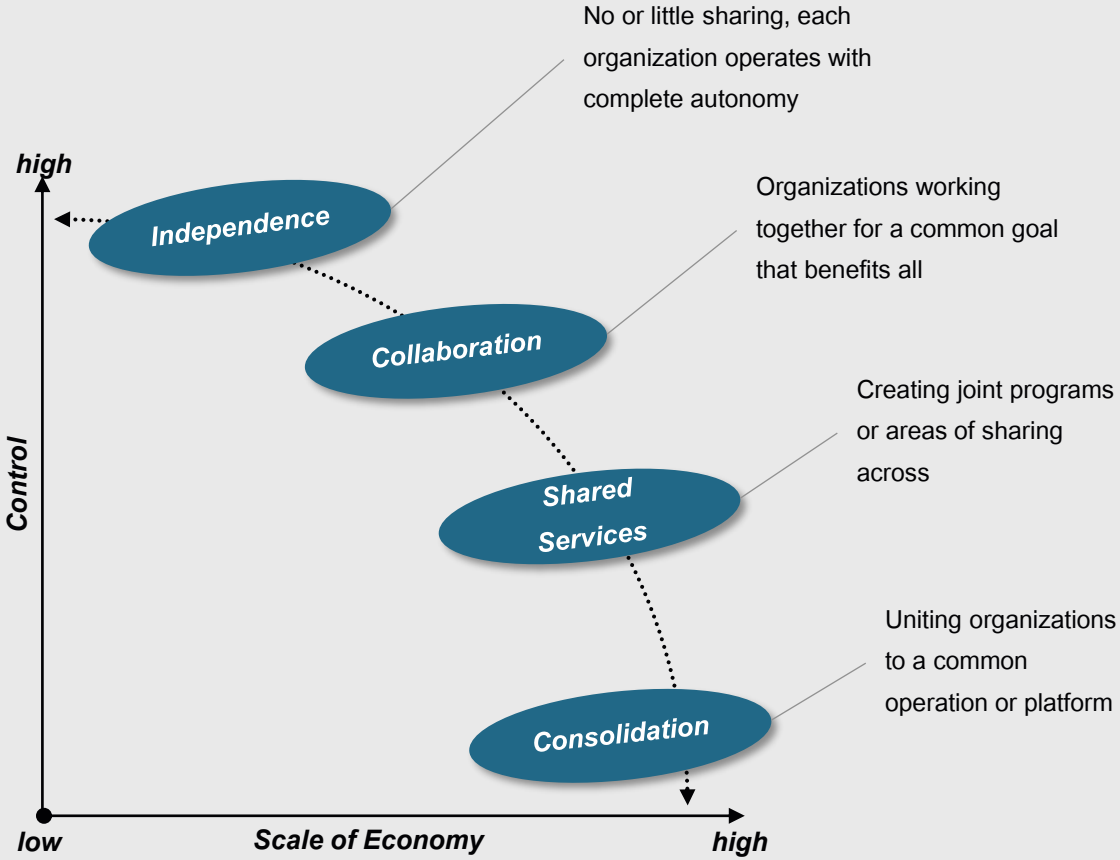
The recommendations support a spectrum of sharing

Any level of sharing should deliver value – cost savings and efficiency of effective of services (e.g. enhanced security)

Any degree of sharing has trade-offs. Various degrees do not require all to participate or move at the same speed, however prerequisites may exist in order to share.

We identified nine opportunities for sharing that cut across all aspects of IT:

- IT Organization – The third-party and IT resources that delivers IT services
- Processes – That IT follows to deliver services
- Architecture – The architecture and standards to govern technology
- Software – User systems that enable the municipality to deliver services
- Hardware – The infrastructure IT supports and maintains



We recommend three transition states that will allow municipalities to join at their own pace

However, if opportunities arise to accelerate a recommendation the municipalities should use judgement to do so

The objective of these recommendations is to increase efficiencies of scale by utilizing shared resources to deliver enhanced services at a reduced cost.

The following pages provide a detailed write-up for each recommendation

- **Situation** – describes the current state and supporting analysis
- **Recommendation** – the proposed solution
- **Actions** – the steps municipalities should take to implement the solution
- **Benefits** – the potential advantages of executing the recommendation
- **Key assumptions** – the assumptions used for quantifying the recommendations
- **Financials** – the cost of implementing the recommendation

	Description	Recommendations
1  **Establish a Foundation**	These activities will help to align member municipalities. Standards and purchasing similar equipment is a requisite for future opportunities in Phase Two.	1. Collaborate on IT strategic planning and innovation 2. Define and implement common standards 3. Pool purchasing power
2  **Expand Collaboration and Sharing**	Once the foundation is set, participating members can take advantage of further benefits of scale.	4. Consolidate IT service agreements 5. Improve network resiliency 6. Consolidate infrastructure 7. Collaborate on system selection
3  **Continue to be Opportunistic**	At any time as opportunities present themselves, take advantage of them on a case by case basis.	8. Migrate workload to the Cloud 9. Leverage project resources

This report describes nine recommendations to improve IT services

The following pages provide a summary of the nine recommendations, the benefits, costs and impact.

Recommendation		Impacted Municipalities	Benefits	Net Impact	One-time Cost
1	Collaborate on IT strategic planning and innovation	All seven municipalities	▸ Shared costs for third party. ▸ More predictable planning can help reduce unexpected costs and identify synergies for future cost savings. ▸ Access to expertise to improve decision-making and risk mitigation.	No financial impact	$50-$75k for a third-party to facilitate and document the plan
2	Define and implement common standards	All seven municipalities	▸ It enables greater sharing and collaboration of the municipalities. ▸ It sets clear expectations for IT delivery organizations or third parties on how to operate. ▸ It improves the security posture of the municipalities.	No financial impact	$20k-$30k for a third-party to assist in developing the standards
3	Pool purchasing power	All seven municipalities	▸ Volume discounts through economies of scale. ▸ Lower cost of IT equipment through negotiating power. ▸ Lower transaction costs associated with purchasing due to the reduced number of contracts prepared and managed by the purchasing group. ▸ Additional financial benefits by improving the refresh cycles of the network and end-user equipment to match industry standards.	$294k decrease in operating costs (over 5 years)	No one-time costs

Note: Net Impact and One-time costs are the total for the impacted municipalities (not for each)

Several opportunities exist to consolidate – from IT managed services to infrastructure

Recommendation		Impacted Municipalities	Benefits	Net Impact	One-time Cost
4	Consolidate IT service agreements	Guelph/Eramosa, Mapleton, Minto, Puslinch and Wellington North	▸ Improved IT services, resiliency and security via hosting servers at a third-party data centre. ▸ Overall reduction in contract costs through a volume discount. ▸ Help to drive greater consistency across the municipalities (e.g. service levels).	Marginal	$50-65k for external expertise
5	Improve network resiliency	Guelph/Eramosa, Mapleton, Minto, Puslinch and Wellington North	▸ Reduce operating costs (e.g. ISP connections). ▸ Improved and standardized service availability, disaster recovery capabilities, resiliency and security.	$120k decrease in operating costs (over 5 years)	$60-$80k for a technical project manager
6	Consolidate infrastructure	Guelph/Eramosa, Mapleton, Minto, Puslinch and Wellington North	▸ Reduced capital costs due to the reduced volume of server replacements. ▸ Reduced administration of duplicate effort for maintenance.	$29k decrease in operating costs and $45k decrease in capital costs (over 5 years)	No one-time costs
7	Collaborate on system selection	All seven municipalities	▸ Shared project costs and management costs (e.g. implementation of Keystone replacement).	$140k decrease in capital costs for each software replacement	$80-100k for external expertise

Note: Net Impact and One-time costs are the total for the impacted municipalities (not for each)

In the next three to five year, software vendors may require municipalities to adopt their Cloud offering

Recommendation		Impacted Municipalities	Benefits	Net Impact	One-time Cost
8	Migrate workload to the Cloud	Centre Wellington, Guelph/Eramosa, Mapleton, Minto, Puslinch and Wellington North	▸ Reduced operating costs associated with server maintenance and management. ▸ Improved security, resiliency and redundancy. ▸ Regular backups, minimizing the risk of losses and eliminates the need for licensing costs.	Potential quantifiable financial impact dependent on specific Cloud migration	No quantifiable costs
9	Leverage project resources	All seven municipalities	▸ It reduces the total cost through synergies by collaborating and leveraging resources on common projects. ▸ It gives municipalities access to resources that they may not have in-house or through their third-party vendor. ▸ It gives municipalities access to projects they may otherwise not pursue due to specialty/niche, high cost or no access to resourcing (e.g. security services).	Potential quantifiable financial impact dependent on project	No quantifiable costs

As per the MMAH, below is the potential cost savings as a percentage of the total amount of service delivery expenditures reviewed.

	Operating Expenditure	Capital Expenditure	Total
Total IT spend of participating municipalities (average 2017-2019)	$4,269,833	$840,660	$5,110,482
Total IT savings	-$443,020 (-10%)	-$185,000 (-22%)	-$628,020 (-12%)

Note: Net Impact and One-time costs are the total for the impacted municipalities (not for each)

We have phased the implementation of recommendations over three years

Below is a proposed implementation plan. Takes into consideration urgency, dependencies and estimated effort. We recommend that following acceptance of this report, the County and participating municipalities commit resources and funding to the recommendations they feel are beneficial, and revise the timeline based on corporate priorities. They should also (where possible) validate the supporting assumptions, develop more detailed implementation plans and create capital projects to implement those recommendations deemed appropriate.

		Relative Timing		
		Year One	Year Two	Year Three
1	Collaborate on IT strategic planning and innovation			
2	Define and implement common standards			
3	Pool purchasing power			
4	Consolidate IT service agreements			
5	Improve network resiliency			
6	Consolidate infrastructure			
7	Collaborate on system selection		As systems need replacement	
8	Migrate workload to the Cloud		As opportunities arise	
9	Leverage project resources		As projects arise	

/ RECOMMENDATIONS

#1 – Collaborate on IT strategic planning and innovation

Situation

Very few of the municipalities operate with a multi-year plan for IT. Most operate using the annual budgeting process to identify next year's projects, capital and operating expenses. In addition, five of the seven rely on a third party to deliver IT services, and only one of the agreements includes multi-year planning or advice on new technology and technology adoption in scope. Consequently, municipalities may not be planning appropriately for the future and lack the expertise to do so themselves.

COVID-19 has also accelerated the need to move more municipal services online / mobile as a lower risk (health risk) option to deliver services (in comparison to in person). This also requires municipalities to digitize (become less reliant on paper) to allow staff to work remotely.

Recommendation

Annually, representatives from the seven municipalities should gather to collaborate on developing a master technology and innovation plan that includes (but not limited to):

- An environment scan (PEST* and trends)
- Summary of business drivers
- Review standards
- Identify collaboration initiatives
- Define a 3-5 year technology plan (list of initiatives by municipality and collective initiatives) including asset refresh

Actions

Step 1: Prep and organize

- Annually, as an input into budgeting process for the municipalities schedule a planning meeting with representatives from the seven member municipalities. The agenda should cover:
  - Scope of the IT strategic plan (develop new or review and modify)
  - Identify topics of interest
  - Inputs to the strategic plan (e.g. current state analysis and trends)
  - The strategic planning session agenda, duration and timing
  - Attendees of the session
  - The need for an independent advisor and their role (purely facilitation or conducting current state analysis, trend analysis and documenting the strategic plan)
- Once agreed, assign action items.

Step 2: Assess the current state

- Establish a template for each municipality to use to assess their current state – business imperatives, current state of IT (architecture, processes, service delivery, spend, etc.), progress on planned initiatives and identify issues / opportunities.
- Where necessary conduct interviews and request data from third parties (for those municipalities that operate with an outsourced IT)
- Populate template and consolidate with others.

*Political, Economical, Social, Technological

#1 – Collaborate on IT strategic planning and innovation

Step 3: Facilitate strategic planning session

- Prior to the session confirm the agenda, and that the necessary preparation activities are complete.
- Conduct the strategic planning session as per the agreed agenda.
- As part of the session, determine the immediate next steps to draft the strategy and the review / signoff process and timeline.

Step 4: Develop IT strategic plan

- Following the session, document the agreed decisions and details. Where necessary gather additional information. See the appendix for a common IT strategic plan table of contents.
- Identify investment requirements and for shared initiatives determine the best way for cost allocation across participating municipalities.
- Once the draft strategic plan is ready, circulate for feedback and refine as per the agreed activities in step three.
- Present to the agreed stakeholders (senior management teams, council).

Step 4: Quarterly progress

- On a quarterly basis, schedule a progress meeting with representatives of the municipalities to provide an update on progress. Discuss any issues / challenges and approach to mitigate. Discuss any changes to the planned initiatives, including any new opportunities.

Step 4: Quarterly progress (continued)

- Use the meeting also for discussing and emerging trends or pilots that were not known at the previous meeting.
- Document and action items and schedule the next quarterly progress.

Benefits

- Cost savings on third party (synergies with facilitation, trend analysis and documenting the strategy).
- More predictable planning can help reduce unexpected costs and identify synergies for future cost savings.
- Access to expertise to improve decision-making and risk mitigation.

Financial Impact

- One-time cost of $50k-$75k for an independent third-party to facilitate (excludes current state analysis) and document the first strategic plan.

Key Assumptions

- After the first strategy is set, subsequent reviews will be done with internal resources only.
- The strategy will describe the ongoing governance that will help ensure progress and alignment of agreed initiatives. It creates the governance (e.g. committees) for other recommendations such as establishing standards.

#2 – Define and implement common standards

Situation

Technology has become widespread and COVID-19 has accelerated our dependency on it. In addition, it is becoming more pervasive as cities move towards becoming 'smarter'. Data collection and transmission continue to grow and consequently the role of security and standards continues to be important. Canadian municipalities are increasingly becoming targets for cybercrime. In 2018, Wasaga Beach and Midland, both in Ontario, 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. 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.

As per industry practices*, organizations should be working towards adopting standards to mitigate risks as well as to help drive consistency. Commonly standards will address security and other areas such as:

► Technology procurement ► Operating Systems ► Identity management	► Data protection loss ► Asset configuration ► Quality assurance / testing	► Cloud use ► Contract / vendor management ► Storage environment

*Control Objectives for Information and related Technology (COBIT - PO3.4 Technology Standards)

As it relates to the seven municipalities, most do not have standards in place. Those that do, have standards that focus primarily on procurement, group policies (e.g. passwords, authentication), anti-virus, and securing network and server infrastructure. Of the seven, only one is performing security assessments on a periodic basis. Standards are not used to guide and govern decision making regarding technology. This is particularly prevalent with municipalities who outsource their IT service delivery.

Recommendation

All seven municipalities collaborate to develop a set of common standards regarding:

- the selection of technology: how each municipality will select, evaluate and procure technology (e.g. desktops, laptops, software)
- the management of technology: how each municipality will secure technology over the course of its lifecycle (including disposal) and
- adherence / enforcement: how each municipality will be held accountable for adhering to the standards

Security and other standards (see table to left) span each of these three areas.

This recommendation sets the foundation for IT shared services. It is a perquisite for most of the other recommendations in this report.

#2 – Define and implement common standards

Actions

Step 1: Establish a committee

- Gather representatives from each municipality that includes various subject matter experts including IT, risk, and procurement.
- Consider using a third party to facilitate the development of the standards.

Step 2: Define the scope of standards

- Develop standards that cover the following areas:
  - Cloud use: the selection and evaluation of using Cloud.
  - Procurement of technology: set an asset lifecycle and where possible characteristics of technology (performance, capacity, etc.). Establish a standard brand (Dell, HP, Cisco, etc.) across the various hardware types and key software (e.g. operating systems, hypervisors and IT tools) assets to drive consistency.
  - Contract / vendor management: oversight, contractual terms and definition of service expectations to manage third party risks.
  - Security: operational and cyber security practices.
  - Controls framework: to ensure adherence to the standards.
- Prioritize these areas to focus the effort on developing the standards. Higher priority should be given to areas where there is similarities (e.g. procurement of desktops and laptops and operating systems) as well as areas of importance e.g. security.

Step 3: Determine the application of industry standards

- Technology standards exist and span the three areas of the recommendation (selection, management and adherence). The municipalities should leverage industry standards to help ensure coverage, alignment with common industry practices and where possible guidance from other government agencies. Examples include:
  - National Institute of Standards and Technology (NIST) framework
  - Control Objectives for Information and Related Technology (COBIT)
  - ISO/IEC 27001
  - ISO/IEC 38500
  - GO-ITS 25.21 Cloud First Principles and Security Requirements
- Use these standards as a basis for defining the standards for the municipalities to adopt. The committee should also focus on what is appropriate given the size and complexity of the various municipalities as well as the risk / value trade-offs.
- Reach out to other municipalities that have been working to better improve their security and technology standards. The City of Stratford for example has partnered with Ryerson University to discuss ways to improve their cyber security capabilities.
- This step concludes with a set of agreed industry practices and details that will help inform the development of standards for the municipalities.

#2 – Define and implement common standards

Step 4: Define common standards

- Use the information from the previous steps to work collaboratively to create a set of standards and revise as required. As the committee develops the standards each municipality should also consider any impacts it may have on other internal policies or practices and develop an action plan to make themselves compliant with the new standards.
- Share standards with IT service provider to understand any other impacts they may cause.
- Once agreed the standards should follow the appropriate approval levels within each organization.

Step 5: Establish adherence (ongoing)

- At this point the committee has established a set of standards and each member municipality has an idea of the changes they must make to align to those standards. The committee will need to then assess the adherence to those standards on an ongoing basis. Initially the frequency should be annual with ad-hoc spot checks.

Benefits

- It enables greater sharing and collaboration of the municipalities
- It sets clear expectations for IT delivery organizations or third parties on how to operate
- It improves the security posture of the municipalities

Financial Impact

- One-time cost of $20k-$30k for an independent third-party to assist in developing the standards.

Key Assumptions

- Approval from senior leadership
- Agreement on standards

#3 – Pool purchasing power

Situation

The municipalities vary in their approach to procure hardware and software.

- One of the municipalities has a Vendor of Record (VOR) with suppliers. This allows for competitive pricing and negotiation.
- Five of the seven municipalities purchase through their third-party IT provider, who mostly purchase directly from vendors. This may prevent these municipalities from receiving reduced prices via the volume discounts that are commonly accessed through a government purchasing groups.
- Two of the seven municipalities purchase through a purchasing group. Purchasing groups are intended to decrease the price of products for their members through greater bargaining power. Purchasing groups typically provide:
  - Savings: through pooled purchasing power and strategic sourcing.
  - Choice: through contracts with multiple vendors that offer a range of options.

The municipalities use many of the same laptop and desktops

- For desktop and laptop equipment the municipalities have similar specifications. However, price vary, as seen in the table to the below. Centre Wellington is purchasing the most cost-effective laptop and desktop models through the OECM purchasing group.

	Laptop			Desktop		
	Vendor	Quote	Main Specs.	Vendor	Quote	Main Specs.
Centre Wellington	Dell	$888	Intel core i5 8GB	Dell	$801	Intel core i5 8GB
County	Dell	$1,162	Intel core i5 8GB	Dell	$803	Intel core i5 8GB
Guelph Eramosa	Lenovo	$1,133	Intel core i5 8GB	Dell*	$1,150	Intel core i7 8GB
Mapleton	Lenovo	$1,600	Intel core i5 8GB	Lenovo	$1,600	Intel core i5 8GB
Minto	Lenovo	$1,900	Intel core i5 8GB	Lenovo	$900	Intel core i5 8GB
Puslinch	HP	$1,323	Intel Core i5 8GB	HP	$1,016	Intel Core i5 8GB
Wellington North	Lenovo	$1,579	Intel Core i5 16GB	Lenovo*	$1,300	Intel Core i7 16GB

Note: * Some specifications vary, that may increase the price, with normalization this would bring them more in-line with the mid-point price.

#3 – Pool purchasing power

The specifications of switches vary among the municipalities

- The table to the right highlights the vendors and models of switches used by each of the seven municipalities. There are few commonalities, such as Cisco 2960, Ubiquiti EdgeSwitch.
- Quotes were provided by most of the municipalities (see table below). While not all quotes included detailed specification of the hardware, it is still clear that there are variances among the price for switches even for like models.

Vendor	Model	Cost
Cisco	2960x	$2,400
Cisco	2960x	$1,680
Cisco	9200	$1,663
Cisco	9300	$2,579
Ubiquity	ES-24-250W	$620
HP	2530	$1,125

	Switch Vendor
Centre Wellington	Cisco
	Fortinet
County	Cisco
Guelph/Eramosa	HP
	Cisco
Mapleton	Ubiquity
	HP
Minto	Ubiquiti
	Cisco
Puslinch	Aruba Net
Wellington North	Cisco
	HP
	Ubiquiti
	Transition

#3 – Pool purchasing power

Asset refresh cycles vary in comparison to each other and industry practices

- IT hardware refresh practices are currently inconsistent across the 7 municipalities (see table to the right).
- The majority refresh on set-frequent cycles, typically every 5 years, and the remainder refresh hardware once they break.
- Common practice is to refresh IT hardware on set-frequent cycles, typically 5 to 7 years depending on the hardware type. While core switches may have a longer life, approximately seven years, the majority of network equipment such as smaller switches, firewalls and wireless access points, five years is an acceptable lifetime

	Desktop	Laptop	Switch	Server
Centre Wellington	4	4	8	5
County	4	4	7	5
Guelph/Eramosa	5	5	5-7	5-7
Mapleton	4	4	5	5
Minto	No refresh cycle. Assets replaced once broken.			
Puslinch	5	5	5-7	5
Wellington North	5	5	5+	6
Industry Practices	*5*	*3*	*5*	*5*

#3 – Pool purchasing power

There are variations in the versions of windows operating systems and Microsoft Office products among the municipalities

- The majority of municipalities are using on-premise versions of MS Office, 2013 or 2016. Both are dated versions of Office that provide limited productivity benefits. MS Office 365 increases staff productivity through the collaboration and remote work tools.

Recommendation

All seven municipalities join a purchasing group (e.g. OECM). Revise procurement policies to allow for bulk purchasing, standardize on common vendors and specifications and align refresh cycles to achieve economies of scale. While not part of our scope, the premise should also be applied to telephony, Internet and mobility.

	MS Windows Operating System			MS Office Version
	Desktop	Laptop	Server	
Centre Wellington	10	10	Various	2013
County	10	10		2016
Guelph/Eramosa	7, 10	10		2013
Mapleton	10	7, 10		365
Minto	10	10		365
Puslinch	7, 10	7, 10		2016
Wellington North	10	10		365

#3 – Pool purchasing power

Actions

Step 1: Conduct a planning session

- Have set the strategic plan in recommendation #1 each municipality has a defined refresh plan for subsequent years.
- Work together to agree on hardware specifications. Given the County and Centre have the largest estates and there is consistency with desktop and laptop specifications they will propose the models (e.g. Dell model XXX laptops, intel i5, 8GB, etc.) for all other municipalities to adopt. The municipalities will be responsible to procure these devices using the agreed purchasing group. This activity must happen on an annual basis as hardware vendors change their specifications and models regularly.
- Identify the municipalities that wish to also migrate to MS Office 365 and include this in the procurement plan.

Step 2: Align refresh cycles

- Adopt the industry practice asset lifecycle. This may cause an increase in cost for some municipalities. It will also require accounting to make changes to the amortization schedule of the assets. Municipalities should phase this in over the next five years to maximize current investments.

Step 3: Identify existing purchasing groups

- Each of the purchasing policies already include a clause for cooperative buying. Specifically, each state that the respective municipality may participate in cooperative purchasing arrangements with other municipalities, County, local boards and public agencies within the Province. This is beneficial, as it means there will be fewer changes to the purchasing policies.
- Conduct research to identify existing purchasing groups (e.g. OECM).
- Reach out to other municipalities within Ontario to discuss whether they are members of existing purchasing groups.

Step 4: Select purchasing groups

- Review the choices of vendors and products that each purchasing group offers. Identify those that align with the agreed upon needs of the group and the newly established purchasing policy.
- Request access to each purchasing group to compare pricing and determine which is the most cost-effective group to join.

#3 – Pool purchasing power

Step 5: Procure

- As hardware and current versions of MS Office requires refresh, have representatives from the committee work with the purchasing group to select equipment and negotiate price.

Benefits

- Volume discounts through economies of scale.
- Lower cost of IT equipment through negotiating power.
- Lower transaction costs associated with purchasing due to the reduced number of contracts prepared and managed by the purchasing group.
- Additional financial benefits may be seen by improving the refresh cycles for some of the network and end-user equipment to match industry standards.

#3 – Pool purchasing power

Key Assumptions

- The following hardware quotes were used for the calculations. We believe that the specifications and models below are reasonable for most of the municipalities.

Hardware	Vendor	Specs.	Cost
Desktop	Dell	Intel core i5 8 GB RAM	$801
Laptop	Dell	Intel core i5 8 GB RAM	$888
Switch	Cisco	9200 24 ports	$1,663

- For the municipalities that did not provide specific age data, we assumed that the hardware to be evenly distributed across all the five years.
- We assume no one-time cost as this will be done with internal resources to managed.
- We were not provided with license costs for the operating systems or MS Office, as such did not include in the analysis.

Financial Impact

- Based on our calculations, the municipalities collectively can save c.$294k over a period of five years. This does not include savings from purchasing other hardware and software.

Financial Impact	Year One	Year Two	Year Three	Year Four	Year Five
Status Quo					
Capital Expenditure					
Desktop	$ 32,855	$ 106,353	$ 113,810	$ 100,325	$ 242,198
Laptop	$ 36,867	$ 98,663	$ 116,075	$ 116,336	$ 271,505
Switch	$ 74,117	$ 39,716	$ 44,375	$ 90,658	$ 79,785
Total Capital	**$ 143,839**	**$ 244,731**	**$ 274,260**	**$ 307,319**	**$ 593,488**
Recommendation					
Capital Expenditure					
Desktop	$ 20,826	$ 102,528	$ 106,533	$ 96,120	$ 221,076
Laptop	$ 24,864	$ 76,368	$ 90,576	$ 87,024	$ 192,696
Switch	$ 54,285	$ 30,766	$ 32,429	$ 77,330	$ 56,542
Total Capital	**$ 99,975**	**$ 209,662**	**$ 229,538**	**$ 260,474**	**$ 470,314**
Net Impact					
Capital savings	-$43,864	-$35,070	-$44,723	-$46,845	-$123,174

#4 – Consolidate IT service agreements

Situation

Five of the municipalities have outsourced their IT to four different vendors, each providing a similar scope of service.*

- The contractual terms vary as highlighted in the table to the right.
- We reviewed each Managed Service Agreement (MSA) assessing 10 key contractual terms and conditions:


Pricing Units


Volume Fluctuation


Scope Definition


Service Levels

Term


Termination


Continuous Improvement & Productivity


Minimum Commitment & Exclusivity


Service Credits


Benchmarking

	Guelph/Eramosa	Mapleton	Puslinch	Wellington North
Contract Cost	$43,320	$33,075	$25,440	$36,742
% of OpEx	47%	34%	38%	39%
Cost/Month /User	$95	$63	$71	$48
Volume	▸ 11 locations ▸ 38 end users	▸ 29 PC's ▸ 2 servers	▸ 20 FTEs ▸ 5 Councillors ▸ 14 workstations ▸ 19 laptops ▸ 1 server ▸ 2 locations	▸ 36 desktops ▸ 6 servers ▸ 21 SPAM filtering
SLA	▸ 24/7/365 critical service monitoring ▸ < 1-hr response for certain services	▸ 24/7/365 network monitoring ▸ Ticket response within 1-hr (business hours)	▸ 24/7/365 network monitoring ▸ < 1-hr response for certain services	▸ 24/7 support - best effort approach
Term	12 months (Jan.1 - Dec.31 2020)	No stated term	12 months (2015)	3 years (2016-19)
Termination	60 days notice	60 days notice	60 days notice	60 days notice

* The executed contract was not provided by the Town of Minto, therefore was not included in the analysis.

#4 – Consolidate IT service agreements

While the MSAs include the following six contractual elements, there are deficiencies relating to scope, termination, volume and cost

	MSA Description		Common Practice
Pricing Units	✓	Some MSAs are fixed price, others are a blend of fixed price plus a variable component. The unit types (e.g. users, PC's, locations) vary. Some of the MSAs explicitly state a unit price, while others do not.	Pricing transparency is fundamental. Without this transparency or linkage to price drivers one party is bearing fluctuation and pricing risk. Commonly, contracts provide a clear separation of costs that specifically outline: 1) a pricing structure that outlines the type (fixed, variable, cost plus), 2) link to services, SLAs and unit prices 3) approach to manage fluctuations and 4) year over year costs.
Volume Fluctuation	✓		
Scope Definition	✓	There are differences in the scope and level of detail among the MSAs – all MSAs include EUE, network equipment and remote support, whereas only some include strategic and budget support. Few of the MSAs scope have a clear linkage to volumes and pricing.	Unclear accountability may lead to confusion between the customer and vendor. We would expect to see 1) service boundaries between the customer and vendor, 2) clear vendor responsibilities and 3) defined link between scope and volume requirements so that price impacts are transparent with no surprises.
Service Levels	✓	There are few or no defined SLAs. Contracts do not include 24-hr response times, and although most of the municipalities operate within 8-5, there are some functions (e.g. recreation facilities) that operate outside those hours that may require 24-hr IT assistance. It is not clear in any of the MSAs how to change SLAs if necessary.	Undefined SLAs can lead to mismatch of expectations and prolonged resolution of issues without any recourse. We would expect to see the MSAs include clearly defined SLAs with mechanisms for making variations to service levels. Typically, there would be a combination of service levels that are quantitative such as response times, and qualitative such as customer satisfaction, innovation and continuous improvement provisions.
Term	✓	The terms vary for each MSA between one to three years. Termination timing varies between 60 days to 6 months. The MSAs do not include specifications for penalties for termination outside notice timeframe, nor do they provide transition plans in the event of termination.	Poorly structured terms, termination and renewals, especially rolling contracts, can lead to vendor complacency and shorter terms often mean higher prices. Commonly, contracts include termination for convenience options exercisable at both the aggregate contract level and for specific services and exit plans and costs are detailed upfront.
Termination	✓		

#4 – Consolidate IT service agreements

Four of the contractual elements are not included in any of the municipalities executed contracts.

		MSA Description		Common Practice
	**CI & Productivity**	✗	The MSAs do not include any of these contractual elements. It is likely, given the size of the vendors that it is not part of their standard terms and conditions and little negotiation occurred. These particular contractual terms are in place to ensure the vendor provides high quality service. Consolidating all five IT contracts into one will give the municipalities more power to negotiate and include these terms, to ensure excellent service.	Additional benefits of outsourcing IT services to a vendor include accessing new capabilities to enhance services and continuous improvement adjustments to service levels. Within the contract, it is common to have clear productivity improvements locked in as contractual commitments.
	**Commitment & Exclusivity**	✗		This contractual element is mostly to help the vendor mitigate risk by requesting a minimum commitment or requesting exclusivity meaning the customer can only use them for that service. While ideal for the vendor, it is generally not recommended for the customer.
	**Service Credits**	✗		This is a mechanism by which an amount is deducted from the contract costs to the vendor if the vendor fails to meet service levels. Typically, the service credits will be based on a “pool amount” that is derived usually as either a portion of the monthly fee or total contact value. Commonly, service credits are allocated to the service levels that are most critical to the business. Contracts will clearly link the service credits to measurable and appropriate service levels. Contracts will include the ability to re-allocate credits to different service levels as business priorities change.
	**Benchmarking**	✗		Benchmarking is optional, it is not necessary for every contract nor every service. The intent is to ensure pricing is in-line with the market. More common is the “Mark to Market” approach, which compares the vendor’s price to the customer against their other customers. Benchmarking exercises occur at least twice in a five-year term and are based on pre-agreed comparators and normalization factors with defined vendor experts. The exercise may result in an adjustment of vendor price to reflect the benchmark after agreed notice period when in customer favour, this can be at the unit/service level or the overall price.

#4 – Consolidate IT service agreements

Recommendation

Consolidate IT services across the member municipalities. The scope of the IT services include:

- Service Desk
- End-user computing
- Infrastructure services
- Data centre facilities
- Network services
- Operational security

Revise the contract terms to be more in-line with common practices.

Pre-requisites

- #2 – Define and Implement Common Standards
- #3 – Pool Purchasing

Actions

Step 1: Form a working group and select an advisor

- Identify representatives from each municipality currently using an outsourced IT service provider. Creating a working group. Consider including representatives from the County and Centre Wellington to assist in this process.
- Select an independent advisor to assist the working group throughout the procurement (requirements gathering, creating an RFP, facilitate the selection and evaluation process).

Step 2: Gather requirements

- Have the advisor gather the service requirements from each participating municipality, i.e. scope of service, service levels, standards (including those from recommendation #2) and any additional supporting information regarding the current state and future projects.
- Ensure the advisor provides templates for capturing the requirements, developing the RFP and supporting RFP articles e.g. pricing form.
- Confirm the commercial option the municipalities desire – one contract for all, and common scope of work, separate contracts, or terms to allow municipalities to exit should they wish.

Step 3: Develop the procurement plan

- Develop a timeline for the procurement that includes the timing of ending current contracts.
- Determine the RFP schedule that aligns with the contracts ending.

#4 – Consolidate IT service agreements

Step 4: Develop and issue an RFP for managed IT services

- Create the RFP, and support RFP templates (pricing, requirements compliance form, financial sustainability questionnaire) for the municipalities, review and revise as required until approved.
- Have the advisor develop evaluation criteria and weighting with input from the participating municipalities. Establish an evaluation team and have the advisor provide an overview of the evaluation process.
- Determine the procurement vehicle to launch the RFP.
- Manage the Q&A from vendors as required.

Step 5: Evaluate Responses and Design future IT operating model

- The advisor should review pricing and perform pricing analysis and where necessary and price normalization.
- Perform the evaluation of the RFP responses.
- The advisor should use the information from the RFP to analyze the details and determine if there is a viable hybrid in-sourcing model (insourcing some of the IT services and perform a cost, benefit and risk analysis. Include IT staff from the County and Centre Wellington as part of the analysis and agree on the best future IT operating model.

Step 6: Select and negotiate

- Having agreed on the future IT operating model, the advisor should proceed review the vendor's standard terms and conditions and work with legal to review to align with industry standards.
- Perform due diligence of the vendor and allow vendor to perform due diligence of the IT estate.
- Once complete, agree on the contract and seek the necessary approvals to proceed with service transition.

Benefits

- Improved IT services, resiliency and security via hosting servers at a third-party data centre.
- Overall reduction in contract costs through a volume discount.
- Help to drive greater consistency across the municipalities (e.g. service levels).

#4 – Consolidate IT service agreements

Key Assumptions

- The cost per user per month for the current MSAs range from $48 to $95, with an average of $69. With volume discounts in effect, the future MSA will be 5% less than the average cost per user per month of the current MSAs.
- The Town of Minto did not provide an executed contract and was therefore not included in the analysis. We would expect the baseline costs to be higher and the savings to be greater if included.
- To perform this work we expect the participating municipalities will require external expertise which would cost $50-65k.

Financial Impact

- We estimate that collectively (across the four municipalities) costs will not change. There may be marginal savings if Minto is also included.

Financial Impact	Year One	Year Two	Year Three	Year Four	Year Five
Status Quo					
Operating Expenditure					
IT MSA	$ 138,577	$ 138,577	$ 138,577	$ 138,577	$ 138,577
Total Operating	**$ 138,577**	**$ 138,577**	**$ 138,577**	**$ 138,577**	**$ 138,577**
Recommendation					
Operating Expenditure					
IT MSA	$ 138,517	$ 138,517	$ 138,517	$ 138,517	$ 138,517
Total Operating	**$ 138,517**	**$ 138,517**	**$ 138,517**	**$ 138,517**	**$ 138,517**
Net Impact					
Operating savings	-$60	-$60	-$60	-$60	-$60

#5 – Improve network resiliency

Situation

Network connectivity is becoming increasingly important for staff and residents. During COVID-19 the need for connectivity became increasingly important and may continue to be important to ensure municipalities are able to communicate and offer services to residents. As such, the need for a more resilient and secure network will be important for municipalities.

- There are 132 networked facilities in total, ranging from 4 to 74 facilities per municipality. This is largely driven by the size of a municipality and number of locations (i.e. degree of disaggregation).
- There is a high degree of varying network resiliency amongst the municipalities.
- In addition, because each municipality has built and operate their own network there is variances across not only the architecture but also the network devices (hardware) and the ISPs as per the table.

	Networked Facilities		ISP
	Total	ISP Connection	
Centre Wellington*	15	2	Rogers HydroOne Wightman
County	74	65	Bell Rogers Wightman + 6 others
Guelph/Eramosa*	5	5	Rogers
Mapleton	5	5	Mornington
Minto	7	7	Wightman
Puslinch	4	3	Rogers
Wellington North	22	2	Packetworks

*Does not include SCADA buildings

#5 – Improve network resiliency

Recommendation

Implement a consistent network architecture for select municipalities (Puslinch, Minto, Mapleton, Wellington North, Guelph Eramosa) and standardize the use of ISPs, having redundant internet connections and segmenting the network traffic.

Pre-requisites

- #2 – Define and Implement Common Standards
- #4 – Consolidate IT Service Agreements

Actions

Step 1: Re-architect the network

- Using the information from this Review gather additional information from the select municipalities' managed service provider.
- Engage resources from the County and Centre Wellington to assist in re-designing a new architecture using a "Hub and spoke" model.
- Create a new standard network architecture and identify the changes necessary to each municipalities network design.
  - Identify for each municipality the primary hub - a location that has access to high bandwidth from multiple ISPs.
  - Identify a site to act as a secondary hub (redundant internet connection) in the event of failure at the primary hub.

Step 1: Re-architect the network (continued)

- Use the security standards identified in recommendation #2 to ensure compliance.
- Standardize the connection between sites by using VLANs between the primary hub and the networked sites "spokes".
- Segment network traffic between municipal traffic and any "guest" traffic e.g. WIFI at recreation or community centres.
- Define the network bandwidth requirements (current and desired)
- For critical infrastructure locations such as SCADA additional resiliency may be required e.g. mobile / cellular connection as a backup solution to ensure connectivity.

Step 2: Go to market

- Using the new network architecture design and pool purchasing, develop an RFP for Internet services.
- Compare the results of the current ISP connections and the results from the RFP. Revise the new network architecture design if the necessary bandwidth is not feasible.
- Select ISPs for all municipalities to use for Internet. Each municipality will have two different ISPs for redundancy in the event of failure.

#5 – Improve network resiliency

Step 3: Build and implement the new network architecture

- Create a project plan to build and implement the new network architecture. The project plan will take into account the current network equipment, the asset refresh cycles, ISP RFP details, budgets and other changes e.g. progress of recommendation #4.
- Begin building the new network architecture by procuring the necessary network devices.
- Configure the network devices as required to conform with security standards and that the devices will automatically re-route traffic via the redundant ISP connection. Work with the municipalities' managed service providers to implement the changes.
- Perform the appropriate testing of the devices and connections.
- Implement the new network as per the plan.

Benefits

- Improved service availability, disaster recovery capabilities, resiliency and security
- Reduce operating costs (e.g. ISP connections)
- Reduce network administration costs

#5 – Improve network resiliency

Key Assumptions

- We assume recommendation #4 has occurred or is happening at the same time. If servers and infrastructure are moved to a third-party data centre, additional redundancy may not be required.
- There will not be reduction in network equipment costs, as each municipal facility will still require them or a replacement depending on the new network hardware standards.
- Adding ISP redundancy will increase the cost slightly for five of the seven municipalities. To calculate this we use an average of the ISP connection cost per location of $885.67/annum.
- All municipalities will pool purchasing power allowing for a 5% volume discount.
- Steps 1-3 will require a technical project manager (contractor) for a year and at a cost of $60-80k.
- We also assume that managed service providers for the municipalities will assist in the project as part of their network service.

Financial Impact

- Based on our calculations, the municipalities collectively can save $120k over a period of five years.

Financial Impact	Year One	Year Two	Year Three	Year Four	Year Five
Status Quo					
Operating Expenditure					
ISP	$ 85,401	$ 85,401	$ 85,401	$ 85,401	$ 85,401
Total Operating	**$ 85,401**	**$ 85,401**	**$ 85,401**	**$ 85,401**	**$ 85,401**
Recommendation					
Operating Expenditure					
ISP	$ 61,292	$ 61,292	$ 61,292	$ 61,292	$ 61,292
Total Operating	**$ 61,292**	**$ 61,292**	**$ 61,292**	**$ 61,292**	**$ 61,292**
Net Impact					
Operational savings	-$24,109	-$24,109	-$24,109	-$24,109	-$24,109

#6 – Consolidate infrastructure

Situation

Each municipality hosts their own servers on premise in their own data rooms or data centres and there a multiple under-utilized assets.

Majority of municipalities use their servers for storage

- The County and Centre Wellington use storage arrays rather than store data on their servers. Both have under-utilized storage as summarized in the table to the right.
- Among the remaining municipalities there are many servers with under-utilized storage. Some servers have as low as 23% storage utilization, while other servers are maxed out at 99%. In total, there is more than 50% free storage space across the 11 servers.
- Some of the municipalities have one server that operates all the municipality's applications. While this can be cost effective it also introduces risk. If the server fails, the municipality will not be able to deliver any of its services.

	Physical Servers	Storage (TB)		Utilization	Range
		Total	Used		
Centre Wellington*	6	63.0	33.0	52%	18-73%
County	13	61.0	24.3	40%	n.a.
Subtotal	19	124.0	57.3	46%	n.a.
Guelph/Eramosa	1	2.70	2.40	89%	n.a.
Mapleton	2	7.48	2.39	32%	23-59%
Minto*	3	2.22	1.87	84%	34-99%
Puslinch	1	5.45	2.89	53%	n.a.
Wellington North	4	6.72	2.78	41%	28-97%
Subtotal	11	24.58	12.34	50%	n.a.
Total	**30**	**148.58**	**69.64**	**47%**	**n.a.**

Note: Storage utilization is calculated as used/total. SCADA servers for both Centre Wellington and Wellington North are not included in the table.

*Storage data was not provided for one of the servers

#6 – Consolidate infrastructure

The municipalities vary in their degree of server virtualization

- Host servers are physical servers that are hosting virtual servers. Some municipalities have all their physical servers acting as host servers, while few municipalities have a low number of host servers, as low as 50%.
- In our review, we were not provided with CPU performance. However, as a rule of thumb, each virtual CPU should map to a physical core. Meaning, that host servers that have more physical cores than virtual CPU, than likely the host server can be further virtualized.
- Virtualization of servers reduces hardware costs by increasing utilization through scalability. Virtual servers are more advantageous than physical servers as they reduce server management effort and downtime by enabling faster application deployment, providing the ability to run different OS, improve disaster recovery and reduce IT maintenance.

#6 – Consolidate infrastructure

Recommendation

Reduce the total number of physical servers through increased virtualization and shared physical servers. There are three options for how the servers could be shared:

1. Smaller municipalities sharing among themselves (Guelph/Eramosa, Mapleton, Minto, Puslinch, Wellington North)
2. The County and Centre Wellington sharing among themselves
3. All member municipalities sharing

However, given the County and Centre Wellington's sophisticated infrastructure set up it would make merging difficult. There we recommend option one.

Pre-requisites

- #2 – Define and Implement Common Standards
- #4 – Consolidate IT Service Agreements

Actions

Step 1: Create a detailed migration plan

- Increase virtualization will allow for two things: a) keeps each municipality's data separate from the others thereby reducing security and privacy risks, b) decreases the volume of physical equipment at the data centre thereby reducing maintenance and overhead costs.

Step 1: Create a detailed migration plan (continued)

- Review the CPU utilization to determine how best to consolidate existing servers. Specifically,
  - Identify all physical cores that are not yet running virtual servers. Use these to host additional virtual servers.
  - Consider the server ages when migrating workloads – move workloads to servers that have been recently purchased and off servers that are older than five years. Ensure that the ages of the remaining servers are evenly distributed across the refresh cycle to lessen the financial burden in a given year.
  - Split each Municipality's servers across multiple physical machines rather than on the same physical server to reduce service disruption caused by potential outages.

Step 2: Migrate the servers

- Virtualize remaining physical servers and onto the new host. Retire the original server. Pick the best time and day that will have the least service disruption, such as evenings and weekend.

Benefits

- Reduced capital costs due to the reduced volume of server replacements and operating costs associated with server maintenance and management.
- Additional savings when combined with opportunity #8. Migrating applications to the Cloud will provide empty space on servers, allowing for further consolidation.

#6 – Consolidate infrastructure

Key Assumptions

- We have modelled option one. Across the five municipalities there 11 physical servers of which eight are hosts to virtual servers and three are additional physical servers.
- The existing eight hosts are running 91 virtual CPU but have a total capacity of 120 cores. As such, the remaining three physical servers can be virtualized onto the existing physical hosts, eliminating the need for three physical servers.
- Additionally, one of the eight host servers is running only two virtual CPU and can be virtualized onto one of the other existing physical hosts.
- Typical maintenance cost per server per month is $95. We assume the cost per server will remain the same in the future.
- Server replacement is spaced out evenly across a five-year refresh cycle in order to distribute the costs.

Financial Impact

- We estimate that the five participating municipalities will collectively save $29k in operating and $45k in capital over a five year period.

Financial Impact		Year One	Year Two	Year Three	Year Four	Year Five
Status Quo						
Operating Expenditure						
Server maintenance	$	12,540 $	12,540 $	12,540 $	12,540 $	12,540
Total Operating	**$**	**12,540 $**	**12,540 $**	**12,540 $**	**12,540 $**	**12,540**
Capital Expenditure						
Server replacement	$	15,000 $	10,000 $	10,000 $	10,000 $	10,000
Total Capital	**$**	**15,000 $**	**10,000 $**	**10,000 $**	**10,000 $**	**10,000**
Recommendation						
Operating Expenditure						
Server maintenance	$	6,840 $	6,840 $	6,840 $	6,840 $	6,840
Total Operating	**$**	**6,840 $**	**6,840 $**	**6,840 $**	**6,840 $**	**6,840**
Capital Expenditure						
Server replacement	$	10,000 $	- $	- $	- $	-
Total Capital	**$**	**10,000 $**	**- $**	**- $**	**- $**	**-**
Net Impact						
Operating savings		-$5,700	-$5,700	-$5,700	-$5,700	-$5,700
Capital savings		-$5,000	-$10,000	-$10,000	-$10,000	-$10,000

#7 – Collaborate on system selection

Situation

The municipalities are using many similar systems.

- Of which, some of the municipalities expressed that they are looking to upgrade or replace two of the systems.
- The municipalities have already partnered with the County to procure and implement the enterprise asset management system, CityWide.

Recommendation

Identify circumstances where municipalities are seeking to replace existing systems and collaborate on:

- Gathering system requirements
- Evaluating and selecting the vendor
- Managing the implementation of the system

Depending on the system, municipalities may choose to collaborate on one, two or all three tasks.

#7 – Collaborate on system selection

Actions

Step 1: Develop a plan

- Having set the strategic plan in recommendation #1, each municipality will have identified which of their systems needs replacement and the timing of the replacement. Working together, identify similar systems among the municipalities and develop a timeline for the procurement that coincides with the desired replacement schedule for all participating municipalities.
- Develop a collaborative procurement plan – will the participating municipalities collaborate on gathering requirements only or will the plan also include going to market and implementing the same system?
- Assign one project manager to represent all participating municipalities.

Step 2: Document system requirements

- Hire a third party that will gather system requirements from each participating municipality. To reduce time and effort, first gather the requirements for one municipality and then bring requirements to the other municipalities to confirm, add or remove requirements.

Step 3: Create an RFP

- Based on the requirements, decide whether to replace the system with the newest version or whether to go to market to find a new solution.
- Have the third party develop one RFP for all the participating municipalities determine the process for procurement, i.e. publish the RFP publicly or invite specific vendors.
- Manage the Q&A from vendors as required.

Step 4: Evaluate responses

- Establish an evaluation team consisting of the third party, project manager and representatives from each of the municipalities.
- Work together to develop evaluation criteria that suits all municipalities. Ensure this includes a demonstration of the solution by the vendors.

Step 5: Select vendor and solution

- Review evaluation scores and pricing. Perform pricing analysis and where necessary, conduct price normalization.
- Determine whether to implement the system together or to sign individual contracts with the vendor.

Step 6: Oversee the implementation across all municipalities

- Create a project team with representatives from each municipality.
- Have the project manager coordinate and liaise with the vendor and the participating municipalities.

Benefits

- Shared project costs and management costs.

#7 – Collaborate on system selection

Key Assumptions

- As Keystone is a potential candidate for upcoming system replacements, we calculated the financial impact for the four municipalities currently using the system. We've assumed this will happen in year one.
- The municipalities will hire a third party to gather requirements, write an RFP and assist in the evaluation. These one-time costs will come out of capital and range between $80-100k.
- We've modelled the impact of labour separately. One municipal representative will conduct project management for all four municipalities and at least four representatives from each municipality will assist in the evaluation of solutions.
- Implementation costs include design, installation, testing, training, etc., all to be completed by an replacement system vendor.
- The licensing costs of the replacement system will be the same, and therefore have not been modelled. However, if the municipalities chose to implement and share the same system there will likely be volume discounts on licenses as well as future savings related to ongoing system maintenance.

Financial Impact

- We estimate that for four municipalities to collaborate on the selection and implementation of one system will save $140k across the participating municipalities.

Financial Impact	Year One
Status Quo	
Capital Expenditure	
Procurement - third party	$ 240,000
Implementation - third party	$ 2,000,000
Total Capital	$ 2,240,000
Municipal Labour Costs	
Procurement - project mgmt.	$ 44,615
Implementation - project mgmt.	$ 160,000
Total Labour Costs	$ 204,615
Recommendation	
Capital Expenditure	
Procurement - third party	$ 100,000
Implementation - third party	$ 2,000,000
Total Capital	$ 2,100,000
Municipal Labour Costs	
Procurement - project mgmt.	$ 29,615
Implementation - project mgmt.	$ 80,000
Total Labour Costs	$ 109,615
Net Impact	
Capital Savings	-$140,000
Labour Efficiency	-$95,000

#8 – Migrate workload to the Cloud

Situation

Cloud computing (Cloud) in its simplest definition is the availability of computer services and applications on demand via the Internet rather than physical on-premise. It provides organizations with a "utility" style service – pay as you go / use and in many cases software vendors will force their customers to use Cloud (see definitions of common Cloud offerings to the right)[1]. The impact of this shift from on-premise to Cloud are:

- Smaller footprint of physical servers and storage
- Need for greater network resiliency and in some cases bandwidth
- Capabilities to manage contracts and vendors versus performing "doing" server upgrades and patching
- Changes to security practices
- Changes to IT expenditure (shift from capital expenses to operating)

With COVID-19, Cloud provides some additional benefits as it relates to accessing the data not only from the office but from home and in the field. It helps organizations with less sophisticated IT infrastructure to provide a resilient service (less downtime, administration and built-in disaster recovery).

Use of Cloud for resident services can also help reduce the risk of disruption.

SaaS	The provider's application is on a Cloud infrastructure. The consumer can access the application from many different client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1. Cloud definitions provided by the National Institute of Standards and Technology (NIST)

#8 – Migrate workload to the Cloud

There are few cases of participating municipalities using Cloud services:

- MS Office 365 – four of the municipalities are using MS Office 365 hosted in the Cloud
- Backups – one municipality is using cloud to backup their data
- SaaS products – one municipality is using Emergency Reporting and ActiveNet, all of the municipalities recently began a joint implementation of the Cloud software CityWide

While Cloud has certain benefits over on-premise it may not always be suitable given the business use, data requirements (criticality and sensitivity) and cost. Both the Canadian federal government and the Ontario government have guidance for adopting Cloud[1].

The collective software inventory for the participating municipalities is over 280 (including different versions)

To focus our assessment of Cloud opportunities we began by:

- Consolidating multiple versions of the same application
- Categorizing the applications as either corporate, business, productivity or IT tools
- Excluding any existing Cloud use, legacy systems, custom-developed, desktop run software, productivity and IT tools

The table below summarizes the candidate workload to migrate to the Cloud by municipality:

	Corporate and Business	Cloud Candidate
Guelph/Eramosa	17	7
Mapleton	6	3
Minto	10	4
Puslinch	7	1
Wellington North	7	2
Total	**47**	**17**

Note: The County and Centre Wellington were excluded from our analysis given their current sophisticated and resilient network architectures. Both municipalities are currently using Cloud and have plans to expand their Cloud footprint.

1. GO-ITS 25.21 Cloud First Principles and Security Requirements

#8 – Migrate workload to the Cloud

We assessed each candidate using our Cloud Assessment Tool

- The tool assesses Cloud potential based on eight criteria:
  - Financial requirements – prefer operating over capital expense?
  - Compliance – does the data need to be in country?
  - Security and risk – what level of security needs to be applied?
  - Technology – is the platform niche or legacy?
  - Capacity/load requirements – are these requirements variable?
  - Operational requirements – is there a strong requirement for automation? Are standardized SLAs acceptable?
  - Latency and bandwidth requirements – are there significant interactions with other systems?
  - Application type – is normal OS/patching control appropriate?
- In cases where SaaS isn't available, the municipalities may consider PaaS if there is a positive financial business case and minimal risk.

#8 – Migrate workload to the Cloud

Recommendation

Move the applications to the Cloud to reduce maintenance and management required for on-premise applications.

- Procure the SaaS product of existing applications in line with their replacement schedules.
- Develop a plan to migrate the remaining municipalities to MS Office 365.
- Where a positive business case exists, migrate the remaining on-premise systems to PaaS.

Pre-requisites

- #1 – Collaborate on IT Strategic Planning and Innovation
- #2 – Define and Implement Common Standards
- #4 – Consolidate IT Service Agreements
- #7 – Collaborate on System Selection

Actions

Step 1: Confirm SaaS Cloud migration opportunities

- Using list of potential Cloud migration opportunities identified, contact the vendors to find out if they offer a SaaS product, what the licensing and the pricing structure.

Step 1: Confirm SaaS Cloud migration opportunities (continued)

- Conduct a Privacy Impact Assessment (PIA) to determine whether there are any privacy risks.

Step 2: Create a replacement schedule

- As part of recommendation #1, update the system replacement schedule that considers:
  - Cloud migration opportunities
  - Date of replacement or upgrade of current systems
  - Vendor plans for the system (e.g. not Cloud now but will be by 2022)
  - Priorities of the organization

Step 3: Procure SaaS Cloud systems

- Conduct a procurement process for Cloud software.
- Include detailed security requirements. Work with your IT provider to identify security needs that may be different now that the system is in the Cloud.
- Use the SaaS vendor and the IT managed service provider to help with the migration from your on-premise solution to the SaaS version.
- Perform the necessary testing to ensure it is operating appropriately.

#8 – Migrate workload to the Cloud

Step 4: Develop a plan to migrate to IaaS or PaaS

- Once the applications are on a SaaS platform, the municipality will require less infrastructure. This will reduce the costs of the future IaaS or PaaS platform.
- Conduct a TCO analysis and PIA for the remaining infrastructure to identify whether there is a positive financial business case and minimal risk. If there is, proceed to develop a migration plan.
- Hire a third-party Cloud expert to assist in the migration. The third party will be responsible for working with the IT provider in establishing the Cloud strategy. This will include defining the Cloud-solution requirements, strategy for data migration and prioritizing the migration.
- In order to have the greatest economic impact, the plan should coincide with the municipality's infrastructure refresh. Working with the third-party expert, build a plan that addresses the following decisions:
  - Single cloud or multi-cloud? Private or public? What should the performance baselines be?
  - The plan should also include a plan for data migration.

Step 5: Revise IT MSA

- Once the municipality is fully in the Cloud, there will be a reduction in labour required from the IT provider. Review the contract to address the change in service.

Benefits

- Reduced operating costs associated with server maintenance and management.
- Improved security, resiliency and redundancy.
- Regular back ups, minimizing the risk of losses and eliminates the need for licensing costs.

#8 – Migrate workload to the Cloud

Financial Impact

There are many factors that need to be considered when calculating the financial impact of Cloud migration. In this section we describe how we would expect current costs to change and provide rudimentary calculations given the data provided.

SaaS – migrating existing applications to the Cloud

- Moving applications to the Cloud will free up current infrastructure. We assessed the impact Cloud migration would have on the current infrastructure.
- These candidates take up a small amount of space on the servers. In order to make a substantial impact to infrastructure costs, the Municipalities would need to move additional applications in order to eliminate entire servers.
- Some additional financial factors to consider include software costs for future Cloud software, labour costs associated with managing the infrastructure and any utility and facility costs.

#8 – Migrate workload to the Cloud

IaaS – migrating the data centres to the Cloud

- IaaS relies on virtual machines, rather than physical. Virtual machines can, in some cases be more cost effective to purchase and maintain compared to physical. For example, in the Azure environment, a virtual machine with 16 cores and 64Gb RAM costs $1,063. In contrast, a physical server with 2 processors, 8 cores and 64Gb RAM can cost over $14,000.
- By moving infrastructure to the Cloud, municipalities can expect to see savings related to administration, facility, energy and third party IT provider costs, specifically reduced labour required by their staff and reduction in their data centre costs. However, there will be one-time implementation costs to cover the migration.
- We used the Azure TCO calculator to assess the potential cost savings over a five-year period of moving your current IT infrastructure to the Cloud. The table to the right provides an example for one of the municipalities.
  - There is a reduction in the hardware costs as physical servers will no longer be used.
  - Software savings come from a reduction in operating system licenses that are associated with the current physical and virtual servers.
  - The municipality will no longer be required to pay for the required electricity.

	On Premise	Azure
Hardware	$76,222	$84,570
Software	$27,215	
Electricity	$9,766	
Virtualization	$9,548	
Data Centre	$22,670	
Networking	$17,852	$17,852
Storage	$1,418	$10,601
IT Labour	$18,401	$17,251
Total	**$183,092**	**$130,274**
Difference	**-$52,818**	

#9 – Leverage project resources

Situation

The municipalities currently engage in some collaboration on projects or project resources (e.g. asset management project). This is primarily because most municipalities do not have dedicated IT resources, and do not have a multi-year IT strategic plan. Given that, there may be missed synergies between member municipalities. As well many of the member municipalities do not have internal IT capabilities and rely on third-parties. This can cause reliance risk and an inability to appropriate challenge the vendors to ensure the solution is fit-for-purpose and meets the needs of the municipality today and in the future. Capacity is also a constraint as the member municipalities tend to have resources that have many responsibilities and therefore projects are some cases secondary to their day-to-day job.

As such, having a method to efficiently collaborate and work together can help to reduce overlap (effort) and in some cases reduce costs if using a third party.

Recommendation

Create a framework that allows for collaborating and sharing resources for IT projects.

Actions

Step 1: Identify areas for collaboration

- Based on recommendation #1 each municipality will have an understanding of potential opportunities for collaboration. Examples include may include:
  - Selecting a third party to perform penetration and vulnerability testing
  - Migrating to MS Office 365
  - Piloting of new smart city innovations
  - Staff education programs to improve technology literacy

Step 2: Establish a framework for collaboration

- Create the framework that will guide the collaboration and sharing of project resources.
- Identify the threshold for collaboration and sharing of project resources, i.e. how many municipalities should be involved before the framework is used? We suggest that if more than two collaborate then the framework be used – this ensures consistency.
- See the following page for the framework details.

#9 – Leverage project resources

Step 3: Establish a framework for collaboration (continued)

- There are three key components to the framework:
  - Scope of service
  - Costing and resourcing
  - Governance and project management
- Note: the governance structure may not be suitable for large complex transformation programs. In those instances the committee should define more specific program management responsibilities and leverage common practices from the Project Management Body of Knowledge (PMBOK) or Managing Successful Programs (MSP).
- Once agreed, the framework should get approved by the member municipalities for use.

Step 4: Execute framework

- As municipalities identify projects to collaborate on, they should adopt the framework and refine as they see fit.

Scope of Service 	► Identify the individual scope of service for each participating municipality. ► Ensure that it captures the needs of all participating municipalities. ► Once the individual scopes have been gathered, identify commonalities and eliminate duplicates in scope. Populate the information into a project charter.
Costing and Resourcing 	► Create a model for cost sharing. Ideally, the cost will break down fixed and variable costs. The former being overhead costs (e.g. PM) and the latter being driven by scope. ► Identify a method for sharing costs based on size of scope. For instance, a simplified model for example purposes may be municipality A's scope is larger by X% due to larger IT environment, therefore the cost ratio is X:1. ► Costs may also include seconding resources from a municipality for a period of time. ► Ensure all participating municipalities are comfortable with the costs and resourcing model.
Governance and Project Management 	► Create a governance model that is based on a committee and committee members from the participating municipalities. ► Establish Terms of References (ToR) for the committee to include frequency, quorum, reporting on the progress, budget and scope. ► That said, identify committee membership based on roles rather than individuals. For example, a committee may include a CAO, IT representative, third-party, and SME (e.g. when procuring an HRIS the SME would be HR). ► Establish project manage practices and outputs. At a minimum it should include: a project charter, a project plan, progress reporting, and risk and issue log.

#9 – Leverage project resources

Benefits

- It reduces the total cost through synergies by collaborating and leveraging resources on common projects.
- It gives municipalities access to resources that they may not have in-house or through their third-party vendor.
- It gives municipalities access to projects they may otherwise not pursue due to speciality/niche, high cost or no access to resourcing (e.g. security services).

Key Assumptions

- Interest in collaborating and sharing resources.
- Approval from senior leadership.
- Agreement on framework.

Financial Impact

- This opportunity does not have a quantifiable financial impact.

/ APPENDIX

Appendix A

Key Municipal Characteristics

	Centre Wellington	County	Guelph/Eramosa	Mapleton	Minto	Puslinch	Wellington North
General Information							
Households[1]	12,918	34,930	4,680	3,280	4,002	3,138	4,870
Land area (Km)[2]	407.54	2,660.57	291.67	534.87	300.69	214.62	526.21
Staffing Characteristics							
Municipal staff (FTE)	209.5	706.0	37.5	44.0	44.0	19.0	64.5
IT staff (FTE)	4.0	21.8	Third party	Third party	Third party	Third party	Third party
Financial Characteristics[3]							
Municipal OpEx[1]	$38,145,383	$224,785,257	$13,420,519	$11,312,546	$13,460,226	$6,565,226	$16,241,624
IT OpEx	$670,277	$3,376,048	$93,903	$100,658	$36,553	$62,277	$103,253
IT OpEx / Municipal OpEx	*1.8%*	*1.5%*	*0.7%*	*0.9%*	*0.3%*	*0.9%*	*0.6%*
Total IT Spend	$934,077	$3,978,048	$115,489	$129,317	$56,102	$117,913	$145,126
Total IT Spend/FTE	*$4,459*	*$5,635*	*$3,080*	*$2,939*	*$1,275*	*$6,206*	*$2,250*
Network Information							
Networked Facilities[4]	15	74	5	5	7	4	22
Managed Network Devices	56	179	29	8	44	6	55

1. Publicly available 2019 Financial Information Return
2. 2016 Statistics Canada
3. 2019 IT operating and capital expenditures provided by individual municipalities
4. Does not included SCADA buildings

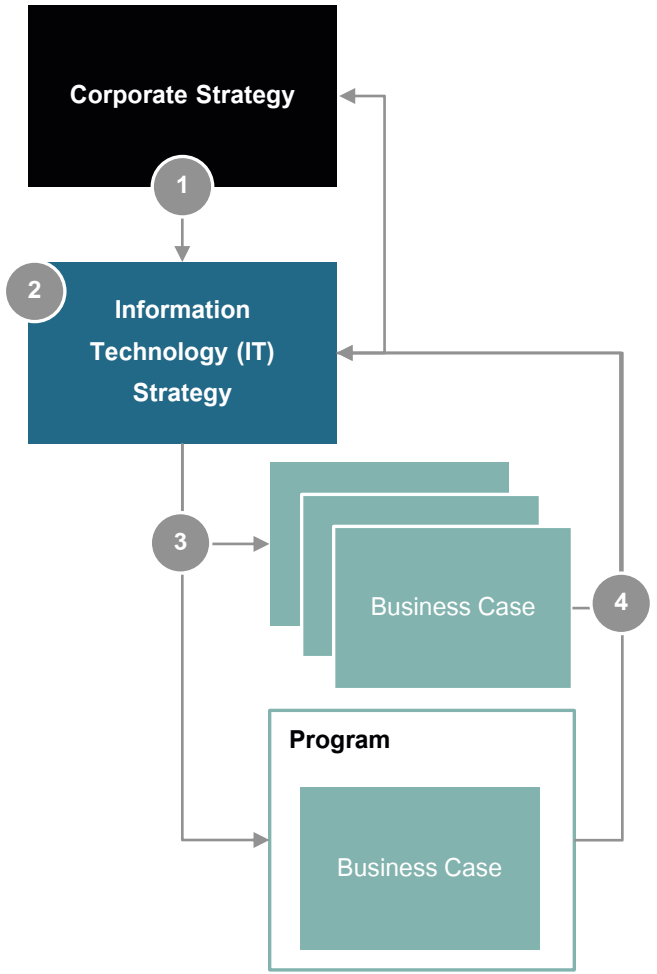
Appendix B

Recommendation #1 – IT Strategic Plan

Below is a brief description of the alignment between corporate strategy, IT strategy and business cases. The right is an illustration.

#	Description
1	Corporate strategic plans typically include a set of goals and priorities that inform an IT or digital strategy
2	An IT strategy typically includes: ► Executive summary ► Influencing factors (internal / external) ► Current situation ► IT Vision and Strategic priorities ► Roadmap ► Detailed Initiatives ► Governance ► Investment Requirements And links (directly / indirectly to the corporate strategic goals / priorities)
3	Once an IT strategy is approved, organizations will typically develop more detailed business cases to then execute the IT strategy and release funding In some cases it makes logical sense to "bundle" projects together into a program. Organizations will either develop project specific business cases and roll it up into a program business case (bottom-up) or the opposite (top-down).
4	The benefits of the business case support the objectives of the IT strategy and / or corporate goals and priorities.

Illustration



Appendix C

Recommendation # 2 – Standards

The following is a set of minimum standards the municipality should consider implementing

Cloud

- Perform a privacy impact assessment prior to using any cloud product
- Data encryption for cloud will be at-rest and in-transit

Hardware

- Network infrastructure is built using <Vendor Name> firewalls, routers and switches and access points
- Servers will be <Vendor Name> with a minimum of XXGB RAM, XX CPU configuration
- Laptops will be <Vendor Name> with a minimum of XXGB RAM, XX CPU configuration – OS will be purchased separately
- Desktops will be <Vendor Name> with a minimum of XXGB RAM, XX CPU configuration – OS will be purchased separately

Security (General)

- Secure communication encryption via Secure Socket Layer (SSL) for web based applications
- All public Internet connections must pass thru a firewall with intrusion detection capabilities
- All laptops hard-drives will be encrypted using <Vendor Name>
- Security education programs for staff will occur annually
- All devices (laptops, desktops, servers, etc.) will have <Vendor Name> Anti-virus and will be kept up to date or unable to connect to the network

Cyber Security

- A cyber response plan will be tested annually
- At a minimum, every two years a vulnerability and penetration test will occur from a third party

Authentication

- Using Single Sign-On (SSO)
  - For internal services, required is LDAP authentication, with a preference for direct SSO using Kerberos
  - For external services, Active Directory Federation Services (ADFS) is to be used
- Administrator level functions are appropriately segregated from user activity, users cannot access or utilize administrator functionality, provide necessary audit and traceability of administrative functionality

Operating Systems (OS)

- Maintain an N+2 on all servers, desktops, laptops and tablets

IT Controls

- Any IT managed service providers must provide an annual attestation report of compliance with the set standards
- Perform annual test of disaster recovery plans
- Create a formal procedure to manage IT incidents
- Create a formal procedure for managing IT changes to minimize operational risk. At a minimum:
  - log changes
  - assess and authorize changes
  - create implementation and roll-back plans
  - conduct testing
  - review roll-out against plan