This report has been prepared by KPMG LLP ("KPMG") for the Corporation of the City of Burlington ("the City") pursuant to the terms of our engagement agreement with the City dated November 18, 2019 (the "Engagement Agreement"). KPMG neither warrants nor represents that the information contained in this report is accurate, complete, sufficient or appropriate for use by any person or entity other than the City or for any purpose other than set out in the Engagement Agreement. This report may not be relied upon by any person or entity other than the City, and KPMG hereby expressly disclaims any and all responsibility or liability to any person or entity other than the City in connection with their use of this report.

AUDIT INFORMATION

Audit Unit: IT Service Support

Service: Information Technology Services

Date Issued: February 7, 2020

Author: Sheila Jones and KPMG LLP

cc: Tim Commisso, City Manager
Laura Boyd, Executive Director Human Resources
Joan Ford, Chief Financial Officer
Allan Magi, Executive Director, Environment, Infrastructure, Community Services
Heather MacDonald, Executive Director, Community Planning, Regulations & Mobility
Nancy Shea Nicol, Executive Director of Services & Corporation Counsel
Kwab Ako-Adjei, Director, Corporate Communications & Government Relations
Nick Anastasopoulos, Director of Building & By-law
Mary Battaglia, Director, Roads, Parks & Forestry
Sue Connor, Director, Transit
Chris Glenn, Director, Recreation Services
Scott Hamilton, Interim Director, Capital Works
Karen Roche, Acting Fire Chief
Angela Morgan, Strategic Lead of Customer Experience
Kevin Arjoon, City Clerk & Director, Clerks
Jamie Tellier, Interim Director, Community Planning
Vito Tolone, Director, Transportation Services

Distribution: Christine Swenor, Chief Information Officer, ITS

Randy Bennett, Manager, IT Infrastructure & Operations

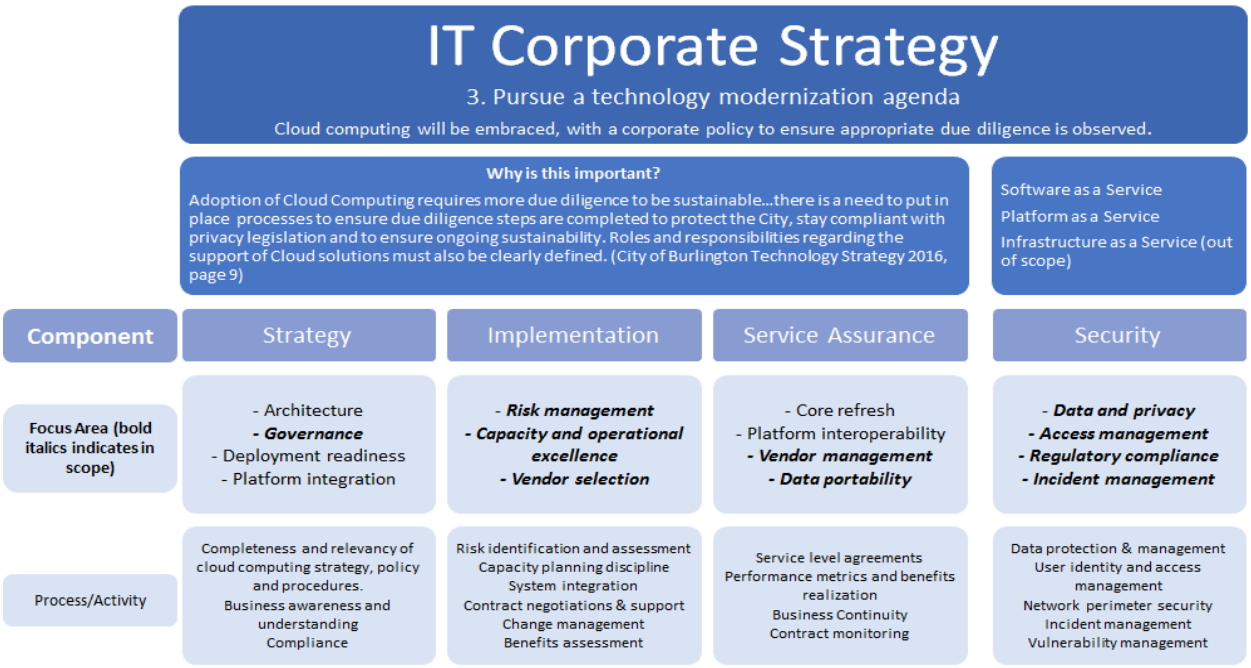
Sef Ullah, Acting Manager, Strategic IT Service Delivery

Wendy Hough, Manager, Business Applications

Ryan Parker, Manager, Information Security

SUMMARY OF AUDIT RESULTS

Area of Focus



Audit Period

Cloud computing applications implemented, in use, and cancelled or decommissioned during the period January 1, 2017 and September 30, 2019.

What is Working Well

- ITS management staff recognize the potential benefits cloud services can bring to the City when risks are managed effectively.
- Cloud Computing Policy and Cloud Computing Framework have been released that provide guidelines to City staff to identify appropriate controls, including security standards and practices required of cloud vendors.

Findings by Severity

(See definitions on Page 15)

Category	Area of Focus	Risk Category	Risk Severity
Strategy	Governance	Performance & Responsibility	Medium
		Performance & Responsibility	Medium
Implementation	Capacity & Operational Excellence	Process	Medium
	Risk Management	Process	Medium

Refer to **Appendix 1** (page 7) for details of the audit findings and recommendations.

Overall Rating

Fair

(See definitions on Page 15)

SUMMARY OF AUDIT RESULTS

Why?
A Cloud Computing Policy and Framework have been designed to address key areas that need to be considered to design controls over Cloud Computing. Awareness, understanding and application of these guiding principles and defined requirements were low among sampled cloud service users. Formalizing, communicating and monitoring of these activities to ensure controls are consistently implemented and operating effectively are lacking.

Closing Comments
We thank management and staff of ITS, Communications, Transit, Environment & Energy, Building & Bylaw, Finance and Customer Service in Recreation Services for the cooperation and support extended to us during this audit.

Management Comments
In recognition of the continued growth of cloud services, IT services management welcomed the opportunity to undertake an audit of the City's cloud computing environment.

The recommendations resulting from this audit will enhance the organization's ability to manage risks and will improve the overall effectiveness in the implementation and sustainability of cloud-based solutions.

IT Services management is appreciative of the thorough and consultative approach taken in conducting this audit.

CITY OF Burlington

DETAILED AUDIT REPORT

IT Services

IT Services provides professional consulting services by proactively assisting the business with technology solutions that meet business objectives. Business relationship management functions as an embedded business partner providing strategic advice and direction on leveraging technology to enhance the business.

IT Services manages a large portfolio of projects varying in size and degree of complexity. Corporate priorities are established by the Burlington Leadership Team and an annual IT project work plan is approved by the corporate IT Steering Committee (ITSC). Work plan adjustments are made throughout the year using a change management process which is managed by the ITSC. IT Services works with customers throughout the life of a project, defining needs, assisting with procurement, and often managing the implementation.

IT services deliver desktop hardware and software support, business application management and support, security, training and general consulting. IT Services is also responsible for managing the City's data centres, network, internet access, email and telephone system.

IT Services manages the life-cycle of all IT assets ensuring ongoing system reliability. IT Services coordinates major upgrades, applies fixes, responds to requests for improvements and provides general support to the user community.

The IT environment is extremely complex and consists of approximately 150 business applications that are delivered through a combination of vendor hosted services and internally delivered applications. IT Services manages contracts and relationships with the IT vendors who supply the systems. A core set of six to 10 systems form the foundation of the City's critical business systems and serve the needs of multiple service areas. IT Services supports application integration to facilitate automated data transfer between business systems.

IT Services staff support more than 1,300 user IDs and over 3,000 devices (including PCs, phones, laptops and servers). IT Services manages all computer-related issues for the City through a centralized service desk and responds to approximately 14,000 incidents and requests each year.

The City's computer network extends to 43 facilities throughout Burlington. A secure internet connection provides access to services outside the City's network.

A comprehensive IT security program plans and implements policies and defenses against IT security threats and vulnerabilities.

IT Corporate Strategy and Service Business Plan

The IT Corporate Strategy sets out a direction to pursue a technology modernization agenda embracing the use of cloud computing with a corporate policy to ensure appropriate due diligence is observed.

More specifically, the Adoption of Cloud Computing requires more due diligence to be sustainable. There is a need to put in place processes to ensure due diligence steps are completed to protect the City, stay compliant with privacy legislation and to ensure ongoing sustainability. Roles and responsibilities regarding the support of Cloud solutions must also be clearly defined. (City of Burlington Technology Strategy 2016, page 9).

The IT service business plans includes, within the anticipated risks section, the challenges with "adoption of vendor hosted solutions: Vendor hosted solutions can help us to be more nimble. However, these externally managed services require staff time to sustain and increase operating costs. Sharing data between hosted systems is frequently a requirement to avoid manual data entry and data duplication. However, facilitating data sharing with hosted applications can be quite time consuming and complex to implement and support. Vendor-hosted services will continue to be a practical option but must be supported by a strong business case that include business benefits and the full cost to sustain the solution."

Cloud Computing Inventory

ITS maintains an inventory of applications hosted on premise and in the cloud. When the inventory of cloud-based applications is merged with the cloud-based application information obtained via survey (for the purposes of this audit), there are 93 known cloud-based applications in use.

Internal Partnerships

IT Service has internal partnerships with every other service.

Audit Objectives

This audit was conducted to assess the design and operating effectiveness of controls in place for Software as a Service (SaaS) and Platform as a Service (PaaS) excluding SAP to assure:

- Compliance with operating policy and procedures (e.g. cloud computing, procurement, privacy, etc.),
- Achievement of business objectives,
- Benefit realization and return on investment,
- Financial sustainability of application, and
- Business continuity.

Audit Scope

Specifically, the review looked on key processes and activities within the following focus areas:

- Governance,
- Risk Management,
- Capacity and Operational Excellence,
- Vendor Management,

- Data Portability,
- Data and Privacy,
- Access Management,
- Regulatory Compliance, and
- Incident Management.

The scope of the review specifically excluded:
- Applications defined as Infrastructure as a Service (IaaS)
- SAP as a Platform as a Service (PaaS),
- Areas of focus including:
    - Architecture,
    - Deployment readiness,
    - Platform integration (the how),
    - Core refresh, and
    - Platform Interoperability.

Role of Management & Inherent Risk

Management is responsible for designing internal controls to lessen the risks in the service or activity and to meet the following objectives:
- Safeguarding of assets (including reputation)
- Compliance with laws, regulations and corporate policies
- Reliability and integrity of financial and operational information
- Efficiency and effectiveness of operations.

APPENDIX 1 – DETAILED FINDINGS, RECOMMENDATIONS & MANAGEMENT ACTION PLANS

Audit Finding #1	**Risk Category:** Performance & Responsibility	**Severity:** Medium

Strategy

Governance

What is happening?
The Cloud Computing Policy ("Cloud Policy") and supporting Cloud Computing Framework ("Framework") have been developed that covers key aspects that need to be considered to manage risks associated with the use of cloud services. The majority of users interviewed were not aware of the Cloud Policy or Framework.

What is the impact?
- Risks may not be managed effectively, and controls are highly reliant on individuals' knowledge and discretion, rather than a formalized consistent approach.
- Services are being used without reference to any of the aspects covered in the Framework and are not registered with ITS as required.
- Non-compliance with internal policies and procedures.
- Increased risk of non-compliance with regulations since controls are informal.
- Enforcement of requirements and holding users accountable becomes more difficult.

Recommendations:
Communication strategy should be developed and implemented that will serve to improve initial awareness and that will reinforce simple and clear requirements supported with the purpose they serve.

Management Action Plan – Audit Finding #1

Comments: Agree

Action Plan:
The existing cloud policy and framework will be updated and will be followed by the development of a communication strategy with the goal of informing and educating on the cloud policy and framework including details on:
- Purpose of the policy and framework
- Roles and responsibility
- How it will be monitored, managed, and enforced

Responsibility: Manager, IT Strategic Service Delivery

Target Date: Q1 2021

Audit Finding #2	**Risk Category:** Process	**Severity:** Medium

Implementation

Capacity & Operational Excellence

What is happening?
Users obtain and use cloud services without registering the services as required with ITS and without demonstrating their consideration of the requirements set out in the Framework.

What is the impact?
- Duplication of effort in the support and management of risks of the same or similar cloud services.
- Unnecessary risks are taken to use additional services, if there are already services in use that have been vetted.
- Ability to respond to or assess the impact of security breaches for particular cloud providers becomes very difficult, when it is not known which cloud services are in use at the City and by whom.
- Increased risk of non-compliance with regulations since controls are dependent on individual users, rather than a centrally managed and considered solution. For example, a lack of compliance to data retention schedules, may lead to data remaining indefinitely on cloud providers' platforms if users do not delete it or leave the City's employment.
- Potential non-compliance to terms and conditions if service providers require different subscriptions products when the number of users per corporation is exceeded or for non-personal use.
- Users who did not register cloud services indicated that they only used these services for public data. However, once the use of a service becomes common, its use and type of data saved may expand to what was initially intended.

Recommendations:
- Enforce the requirement to have cloud services registered with ITS.
- Based on registered services, maintain an inventory of cloud services used. At a minimum the inventory of registered services should indicate its use, the type of data stored and the business owner.
- Review the cloud services offered periodically to identify opportunities to consolidate services, identify where services provided internally do not meet users' needs or where training in existing services are required.

Management Action Plan – Audit Finding #2

Comments: Agree

Action Plan:
The following actions will be taken in response to the recommendation:

- A process for registering cloud applications will be implemented and will form the basis for updating the existing application inventory.
- The application inventory will include but not be limited to a description of the system, any confidential/private data stored, security assessments or PIA's performed, key contacts in IT Services and the business.
- The inventory will be shared with the business on an annual basis to confirm the solution is still in use and the information on file is accurate
- Opportunities to consolidate cloud services may be considered within the scope of larger software implementations and/or within regular planning discussions between ITS and the business
- The inventory will form the basis for defining acceptable cloud applications and will be published as such

Responsibility: Manager, Business Applications; Manager, IT Strategic Service Delivery

Target Date: Q1 2021

APPENDIX 1 – DETAILED FINDINGS, RECOMMENDATIONS & MANAGEMENT ACTION PLANS

Audit Finding #3	**Risk Category:** Process	**Severity:** Medium

Implementation

Risk Management

What is happening?
The Framework covers key areas but does not suggest minimum requirements or provide specifics to help business owners know what level of controls are effective. For example, the framework suggests "the vendor has some redundancy" but to a business owner it may not be clear what is required. Also, the Framework does not provide for a process of dealing with areas that will not be addressed, for example where the business may decide to accept a risk. Roles and responsibilities to ensure that processes are in place are working are not defined.

What is the impact?
- The lack of a definition of what constitutes an effective level of control may lead to inconsistent or weak control mechanisms. Risks may not be managed effectively. Conversely, too much control and effort may be spent on services that pose little to no risk.

Recommendations:
- A standardized risk assessment methodology should be created that includes a list of typical risk factors and used to help identify the level of risk that needs to be managed and help classify cloud services accordingly. Risk factors could be based on factors such as: the level of dependence on the services for business critical processes, whether the service will be customer facing, the number of users using the service, data classification or level of reliance on the data.
- As part of the defined risk methodology, prescribed minimum controls and standards should be linked to risks. For example, if personally identifiable data is present, a Privacy Impact Assessment must be conducted.

Management Action Plan – Audit Finding #3

Comments: Agree

Action Plan:
A risk assessment methodology will be developed and will be used to classify cloud services. It will include relevant risk factors and will prescribe new controls to mitigate the risks. Additional follow-up work including conducting Security and Privacy Impact Assessments will require additional time and resources from IT Services and the City Clerks Office.

Management Action Plan – Audit Finding #3 (continued)

Responsibility: Manager, Information Security

Target Date: Q2 2021

Audit Finding #4	**Risk Category:** Performance & Responsibility	**Severity:** Medium

Strategy

Governance

What is happening?

The Framework provides guidance at a high level in terms of management of cloud services. Specific monitoring activities to be performed on a periodic/ongoing are not defined. For example, changes in terms and conditions, privacy statements subsequent to the initial vetting process are not considered, nor are there prescribed requirements for user access revalidations to be performed by business owners and processes determined to modify/revoke access based on changing user roles within the City.

What is the impact?

- Control activities may not be performed at all.
- When roles change, or individuals leave, activities previously performed may not be continued, especially in areas where support responsibilities are shared between business and ITS.
- If it is not known whether processes are working, actions cannot be taken to improve processes or take corrective actions.
- Individuals are less likely to comply with policies and follow defined process when it is known that no follow-up process in place.

Recommendations:

- Define prescribed cloud control activities and who needs to perform them for each cloud service. Develop an application support model that includes specific process areas such as user access management, vendor management, terms and conditions, requests and incidents handling, and who is responsible for controls review over the duration. The level of detail can be determined using the classification system above, e.g. predefined activities.
- Monitoring controls are needed to determine whether the processes that are in place are working and are effective.
- Enforcement of policies and procedures, mechanisms to follow-up and enforce. Requirements should be clear, and it should also be clear that compliance is enforced.
- Monitor and review existing applications that may evolve over time (e.g. where the uses of the app are expanded, or where new information/data is introduced or linked within the app) as changes may necessitate introduction of new or modification of existing controls/practices.

Management Action Plan – Audit Finding #4

Comments: Agree

Action Plan:
IT Services will develop and update existing application support models identifying cloud control activities that need to be performed. The support models will initially focus on cloud services that are classified as high risk followed by medium risk services. The application support model will identify the specific responsibilities that reside within the business and those that reside within IT Services for cloud control activities that need to be performed. Given the number of cloud services in place and the current operational workload in IT Services this work will take several months and may require additional staff resources to maintain and enforce the operating model and/or require assistance from 3rd party resources.

Addressing the recommendations in this finding will require new or updated operational processes that will impact the responsibilities of both IT Services and business staff.

Responsibility: Manager, Business Applications; Manager, Information Security

Target Date: Q4 2021

APPENDIX 2 – ADDITIONAL OBSERVATIONS

Additional Observation #1

What is happening?
The Framework lacks integration of components with acceptable use and technology security policies and does not define responsibilities of an IT security manager, nor are all terms defined. Requirements for registration of new cloud services with ITS may not be prominent enough in the Framework and Policy.

Recommendation
The Framework should be reviewed, and minor updates considered. References of "value for money" should be reconsidered. Technology Acceptable Use and Information Technology Security Policies should reference the Cloud Policy. Alternatively, to simplify requirements and the number of policies, management should consider adding cloud policy statements or requirements within other policies, such as the Technology Acceptable Use.

The requirement of registering new services with ITS in the Cloud Computing Policy is currently included in the Scope section. Specific requirements should be included as part of the Policy Statement or a dedicated section.

Roles referenced in the Framework should be reviewed and additions made, such as the role of IT security manager in the roles and responsibilities section. Links and definitions should be updated, for example the reference to the guideline on page 5 of the Cloud Policy. The definition of Personal Cloud Service should be completed on page 13 of the Framework.

LEGENDS & INTERNAL AUDIT STANDARDS

Overall Audit Ratings	
Rating	**Description**
Excellent	• No internal control weaknesses noted. • Good adherence to laws, regulations, and policies. • Good control environment. • Operations are considered efficient and effective.
Good	• Several low and/or one or two medium findings. • Minor contraventions of policies and procedures with compensating controls in place. • No violation of laws. • Minor opportunities for improvement in efficiency and effectiveness.
Fair	• Many medium findings and/or one or two high findings. • Several contraventions to policy. • Minor violations of regulations/laws with minimal impact to City. • Moderate opportunities for improvement in efficiency and effectiveness.
Weak	• Several high findings and some medium and/or low findings • Controls weak in one or more areas. • Noncompliance with policies put the City at risk. • Violation of law/regulation put the City at risk. • Substantial opportunities for improvement. • Operations are considered consistently inefficient and/or ineffective

Audit Finding Severity Scale	
Severity	**Details**
High	• Residual risk is very high or high • Key control does not exist, is poorly designed or is not operating as intended • Serious non-compliance to policy or regulation • May result in immediate or material loss/misuse of assets, legal/regulatory action, material financial statement misstatements, etc. • Indicates a serious business control weakness/deficiency requiring immediate action
Medium	• Residual risk is medium • Key controls are partially in place and/or are operating only somewhat effectively • Some non-compliance to policy or regulation • May negatively affect the efficiency and effectiveness of operations and/or financial reporting accuracy. • Indicates a business control concern requiring near-term action be taken
Low	• Residual risk is low to very low • Key controls are in place, but procedures and/or operations could be enhanced. • Minor non-compliance to policy or regulation • May result in minor impact to operations. • Indicates a business control improvement opportunity for which longer-term action may be acceptable.

Audit Methodology

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing. The City Auditor relied upon interviews with and observation of key personnel, examination of information, data, and other documentary evidence and re-testing of controls.

Audit Conclusions

The conclusions reached in this report are based upon information available at the time. The overall conclusion is only applicable to the function/area of this audit. It reflects the professional judgment of the Office of the City Auditor based on a comparison of situations as they existed at the time against audit criteria as identified in the scope of the audit.

Reasonable Assurance

This conclusion is intended to provide reasonable assurance regarding internal controls. There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls may provide only reasonable assurance with respect to City operations.