brampton.ca BRAMPTON Flower City

Agenda

Audit Committee
Committee of the Council of
The Corporation of the City of Brampton

Tuesday, March 19, 2019
9:30 a.m. – Regular Meeting

Closed Session (See Item 10) – Following Regular Business
(Under Section 239 of the Municipal Act, SO, 2001)

Council Chambers – 4th Floor – City Hall

Council Members:	Regional Councillor M. Medeiros – Wards 3 and 4 (Chair) Regional Councillor R. Santos – Wards 1 and 5 (Vice-Chair) Regional Councillor M. Palleschi – Wards 2 and 6 Regional Councillor G. Dhillon – Wards 9 and 10 City Councillor J. Bowman – Wards 3 and 4 City Councillor D. Whillans – Wards 2 and 6 City Councillor H. Singh – Wards 9 and 10
Citizen Members:	Iqbal Ali Rishi Jain Abid Zaman

For inquiries about this agenda, or to make arrangements for accessibility accommodations for persons attending (some advance notice may be required), please contact:

Sonya Pacheco, Legislative Coordinator
Telephone (905) 874-2178, TTY (905) 874-2130, cityclerksoffice@brampton.ca

Note: Meeting information is also available in alternate formats, upon request.

Note: Any difficulty accessing meeting rooms, buildings, elevators, etc. please contact security at 905-874-2111

1. Approval of Agenda

2. Declarations of Interest under the Municipal Conflict of Interest Act

3. Consent

* The following items listed with an asterisk (*) are considered to be routine and non-controversial by the Committee and will be approved at this time. There will be no separate discussion of any of these items unless a Committee Member requests it, in which case the item will not be consented to and will be considered in the normal sequence of the agenda.

(nil)

4. Delegations/Presentations

4.1. Presentation by F. Velji, Director and Chief Audit Executive, Office of Internal Audit, re: **Corporate Fraud Prevention Hotline Update**.

(See Item 5.4)

5. Reports – Internal Audit

5.1. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated January 8, 2019, re: **Update of the Internal Audit Charter and Audit Committee Terms of Reference**.

Recommendation

5.2. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated January 2, 2019, re: **Internal Quality Assessment Review Results**.

To be received

5.3. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated February 7, 2019, re: **Status of Management Action Plans – December 31, 2018**.

To be received

5.4. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated January 7, 2019, re: **Corporate Fraud Prevention Hotline Update**.

(See Item 4.1)

Recommendation

5.5. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated February 5, 2019, re: **Internal Audit Work Plan – 2019**.

To be received

5.6. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated November 30, 2018, re: **IT Service Desk Audit Report**.

5.7. Report from F. Velji, Director and Chief Audit Executive, Office of Internal Audit, dated November 30, 2018, re: **Mobile Phone Management Follow-Up Audit Report**.

To be distributed prior to the meeting

6. Reports – Finance

7. Other/New Business

8. Question Period

9. Public Question Period

15 Minute Limit (regarding any item decision made at this meeting)

10. Closed Session

Note: A separate package regarding these agenda items is distributed to Members of Audit Committee and senior staff only.

10.1. The security of the property of the municipality or local board

11. Adjournment

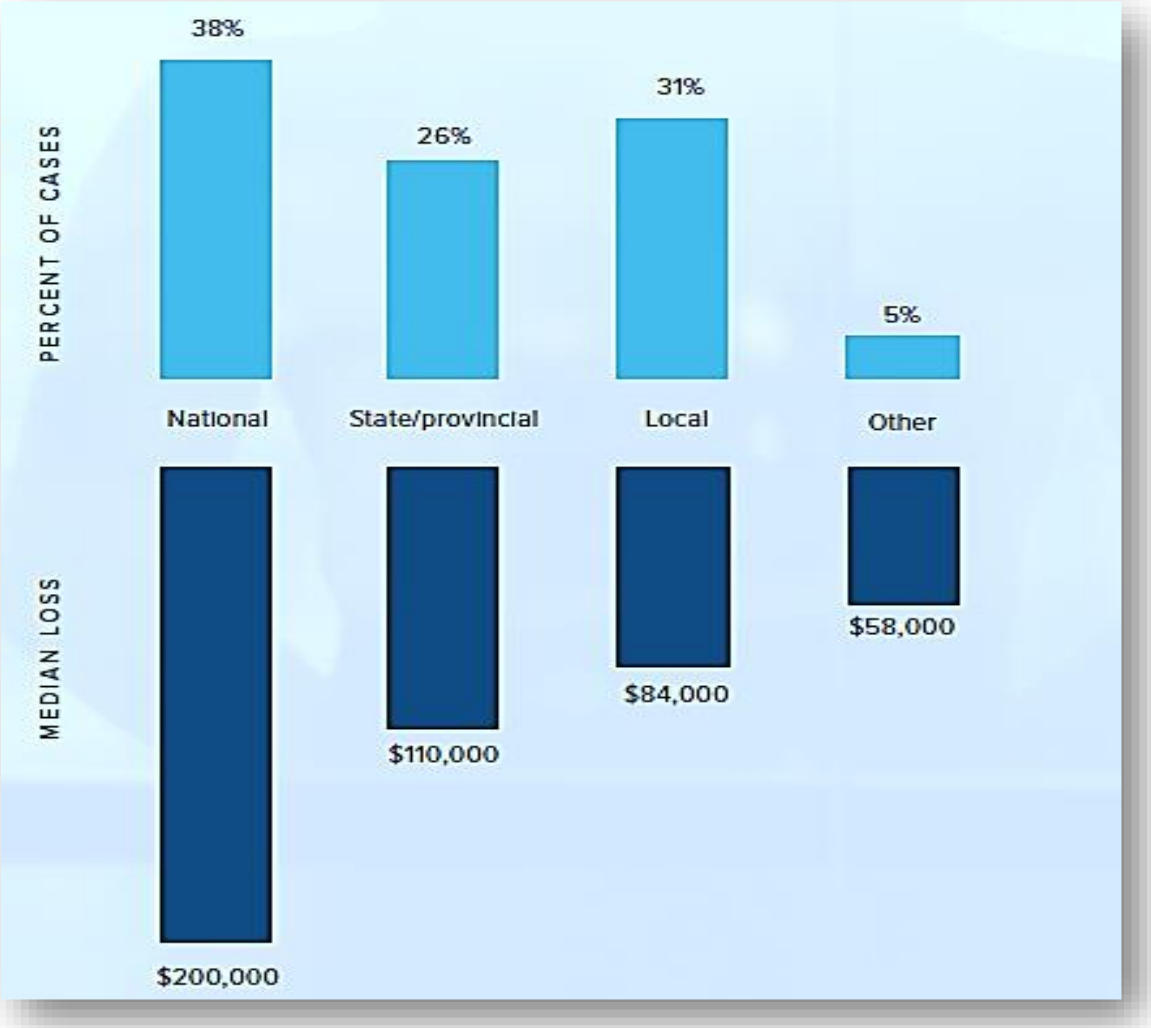
Next Meeting: Tuesday, June 11, 2019 at 1:00 p.m.

CORPORATE FRAUD HOTLINE UPDATE
Council Presentation
March 19, 2019

Foruzan Velji, Director
Office of Internal Audit

Levels of Government victimized by Fraud

2018 Report to the Nations on Occupational Fraud and Abuse-Government Edition



Fraud Detection Methods

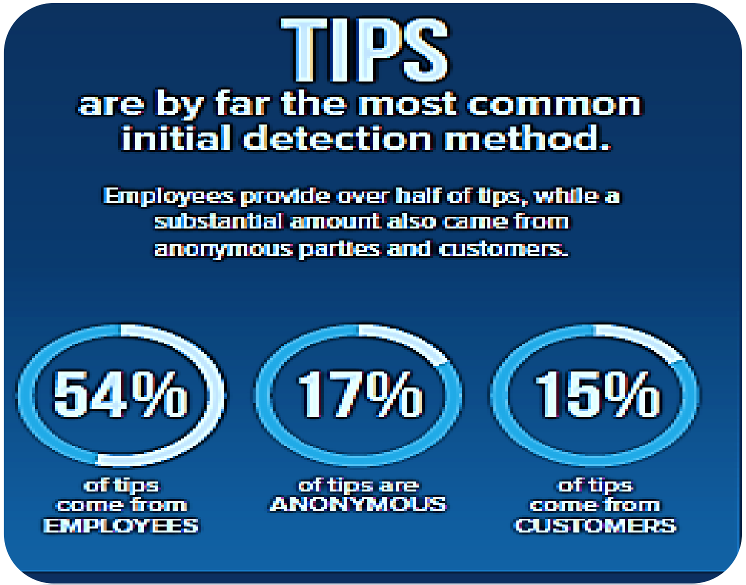
2018 Report to the Nations on Occupational Fraud and Abuse

- Tips are the most common detection method.
- More cases of fraud in government were discovered through tips than by the next six detection methods combined.

Method	% GOV	% CDA
Tip	45	32
Internal Audit	15	21
Management Review	9	15
Account Reconciliation	4	5
By Accident	4	4
Other	5	7
Document Examination	4	4
Surveillance/Monitoring	2	6
IT Controls	1	1
External Audit	6	5
Notified by Law Enforcement	5	n/p
Confession	1	n/p

Fraud Hotlines and Reporting Mechanisms

- Most common



TIPS

are by far the most common initial detection method.

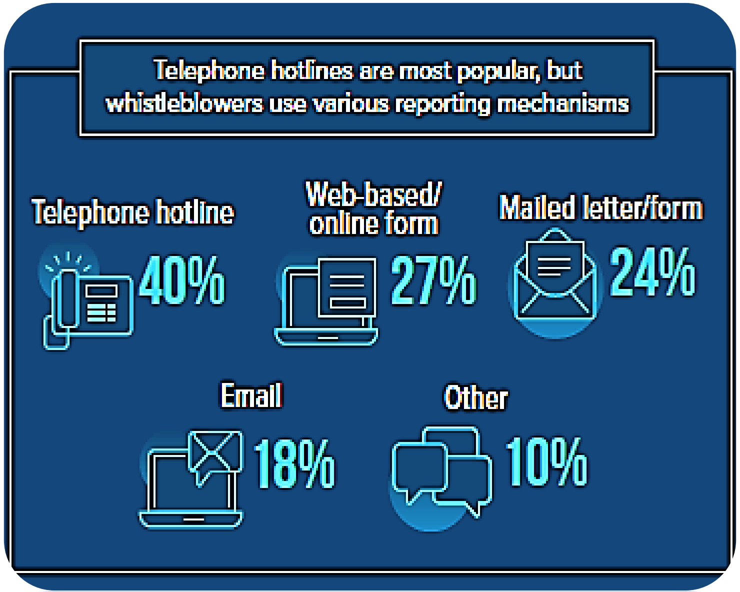
Employees provide over half of tips, while a substantial amount also came from anonymous parties and customers.

54% of tips come from EMPLOYEES

17% of tips are ANONYMOUS

15% of tips come from CUSTOMERS

- Hotlines



Telephone hotlines are most popular, but whistleblowers use various reporting mechanisms

Telephone hotline	Web-based/ online form	Mailed letter/form	Email	Other
40%	27%	24%	18%	10%

Background

- City of Brampton is committed to protecting its assets and to the principles of accountability and stewardship of public funds
- Established a framework to prevent, detect and report incidents of fraud; and a process to investigate and report on fraudulent acts
- Framework
  - Includes **Corporate Fraud Prevention Policy** and **Fraud Hotline**
  - Complements existing City of Brampton policies
- **Fraud Hotline**
  - Initially launched in July 2016
  - Underutilization of Hotline due to lack of staff awareness
  - Relaunched in March 2018

Revised Corporate Fraud Prevention Policy

✓ **Approved** by Council March 1, 2018

✓ **Applies** to all persons employed by or acting on behalf of the City

☐ Key components:

- No person shall commit fraud
- Defines fraud and gives examples
- Immediate reporting of suspected fraud
- No retaliation against whistleblower
- **Everyone is responsible for reporting fraud or any contraventions to the Employee Code of Conduct**
- Outlines additional responsibilities of employees/managers to detect and prevent fraud
- Consequences ➔ Discipline up to **termination**

Fraud Hotline

Vendor

CLEARVIEW CONNECTS™

CLEARVIEW™ STRATEGIC PARTNERS

Clients

BMO

TTC

LCBO

Region of Peel

OLG

Bell

THE CITY OF CALGARY

Ottawa

CANADA POST POSTES CANADA

MISSISSAUGA Leading today for tomorrow

OAKVILLE

Goal – City of Brampton Culture Where:

- All employees live our values of integrity, courage, trust and compassion
- All employees take responsibility and do the right thing
- All employees are treated fairly, with dignity and respect
- Workplace is open, transparent and staff at all levels are accountable for their actions
- Staff are aware of and understand their role and responsibility in identifying and reporting instances of fraud or any contraventions to the Employee Code of Conduct

Activities Completed

March 1 to December 31, 2018

✓ **34** Fraud Presentations by the Office of Internal Audit:

Department	**8**
Division	**18**
All Staff	**8**

✓ **9** Fraud articles issued (2 in collaboration with Human Resources)

✓ Corporate Fraud Prevention Policy approved by Council

✓ Fraud Poster – **BE A HERO. Speak up with Confidence**

✓ Poster and Quiz Contest for **International Fraud Awareness Week**

✓ Fraud Policy signoff form for new staff onboarding

✓ Fraud Investigation SOP

Fraud Prevention Month is March

- Presentations to be done:
  - Division 14
  - All Staff 21

- Articles in ***Connections*** and on ***OurBrampton.ca*** portal
  - Fraud Red Flags
  - Fraud Triangle
  - Fraud information in upcoming Recreation and Transit Department Newsletters

- Developing material for Fraud Prevention Month

Critical to Success ➔ What we need from you

Now and Ongoing

- Strong and Consistent “Tone at the Top”
- Evidence of Support for Fraud Prevention Program, Fraud Hotline and related initiatives by:
  - ✓ Endorsing revised Corporate Fraud Prevention Policy
  - ✓ “Walking the talk”
  - ✓ Promoting and encouraging culture of “If you see something, say something.”

QUESTIONS?

CONTACTS:

Foruzan Velji 905-874-2215

Report

Audit Committee

The Corporation of the City of Brampton

March 19, 2019

Date: January 8, 2019

Subject: **Update of the Internal Audit Charter and Audit Committee Terms of Reference**

Contact: Foruzan Velji, Director, Office of Internal Audit, 905-874-2215, Foruzan.Velji@brampton.ca

Recommendations:

1. That the report from Foruzan Velji, Director, Office of Internal Audit, dated January 8, 2019, to the Audit Committee Meeting of March 19, 2019, re: **Update of the Internal Audit Charter and Audit Committee Terms of Reference**, be received;

2. That the updated Internal Audit Charter Version 2019, as set out in Appendix 1 to this report, be approved; and

3. That the updated Audit Committee Terms of Reference Version 2019, as set out in Appendix 3 to this report, be adopted.

Overview:

- The Office of Internal Audit is committed to review the Internal Audit Charter and the Audit Committee Terms of Reference on an annual basis and update either document if necessary.
- The Internal Audit Charter 2019 version has amendments to increase the clarity of the Internal Audit Charter as well as increase the readability of the document. It should be noted that the Internal Audit Charter 2017 was aligned with the IIA *Standards* and *Code of Ethics*.
- The draft Terms of Reference for the 2018-2022 Audit Committee was presented and endorsed at the February 2018 Audit Committee meeting. This February 2018 draft was amended to include citizens as members of the Audit Committee.

Background:

The Audit Committee was established in 2002 to provide enhanced oversight capabilities and stewardship responsibilities of Council. At that time the Internal Audit Charter and the Committee's Terms of Reference were presented to the Committee.

The Office of Internal Audit is committed to review the Charter and the Terms of Reference at the beginning of each term of Council and update either document if necessary. In addition, the Director, Office of Internal Audit reviews the Internal Audit Charter annually to determine if significant changes are required based on changes to the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing (*"Standards").*

The Internal Audit Charter was last updated and presented to Audit Committee at the September 12, 2017 Committee meeting. The revisions to the Charter at that time were to reflect changes to the *Standards* that had come into effect on January 1, 2017. The *Standards* have not changed since January 2017.

The Audit Committee Terms of Reference were last updated and approved by Council on September 27, 2017 to further enhance the independence of Internal Audit.

Current Situation:

Internal Audit Charter update Version 2019

The objective of the Internal Audit Charter is to outline the purpose and mission, authority, scope and responsibilities of the Office of Internal Audit and ensure they are consistent with the *Standards*.

The Charter establishes the Office of Internal Audit's position within the City of Brampton, special interest groups and related Boards, including the nature of the Chief Audit Executive ("CAE") functional reporting relationship with the Audit Committee; authorizes access to records, personnel, and physical properties relevant to the performance of projects. Essentially, the Charter serves as a guide for Internal Audit in the performance of its duties.

The Charter also outlines that the internal audit activity is performed in an independent and objective manner.

One of the Office of Internal Audit's Divisional Goals for 2018 was "Establishment as a Leader in Internal Audit." Updating the Charter was part of that goal. The Charter was reviewed against best practices and guidance from the IIA for Internal Audit Charters. As a result, three areas were identified where additional language would provide greater clarity.

- *Independence and Objectivity*: text was added to provide details of what would constitute situations where independence would be impaired. Text was also added to provide details of staff level, versus CAE level, responsibility to maintain their independence and objectivity.

- *Reporting of the CAE to the Audit Committee*: detail was added from the *Standards* on what specifically the CAE will report on. These specific reporting responsibilities are set out in different parts of the Charter. Listing them together in one area provides an overview of what should be reported to Audit Committee, and conversely what Audit Committee is tasked to review as set out in its Terms of Reference.

- *Responsibilities of the CAE*: two areas were added. Ensuring policies and procedures for the Internal Audit activity are in place and adhered to, as well as adherence to the City's policies and procedures. Both of these points were captured by language in the *Standards* paragraph in the previous Charter.

Audit Committee Terms of Reference Version 2019

The Terms of Reference outlines the objectives and responsibilities of the Audit Committee. The Committee's responsibilities include both internal and external audit activity.

The Terms of Reference Version 2019 is unchanged from the version presented for review at the February 2018 Audit Committee. The February 2018 version was amended to reflect the inclusion of one to three citizen members as part of the Audit Committee.

The Terms of Reference did not require any updating from the previously endorsed February 2018 version and is presented to Audit Committee as the 2019 Version.

Corporate Implications:

Financial Implications:

N/A

Other Implications:

N/A

Strategic Plan:

This report achieves the Strategic Plan priorities for Good Government by ensuring that best practices are reflected in the Office of Internal Audit's Charter and the Audit Committee's Terms of Reference.

Conclusion:

The Office of Internal Audit performs its work independently and objectively. Enhancements to the Internal Audit Charter will ensure that Internal Audit continues to provide the highest quality of value-added service to the City of Brampton.

Approved by:

Foruzan Velji, CPA, CA, CIA, CISA
Director, Office of Internal Audit

Attachments:

Appendix 1: Internal Audit Charter Version 2019 – Clean
Appendix 2: Internal Audit Charter Version 2019 – Marked
Appendix 3: Audit Committee Terms of Reference 2019 – Clean

Report authored by: Ella Kila, CPA, CA
Senior Advisor, Office of Internal Audit

Appendix 1

5.1-5

Corporation of the City of Brampton
The Office of Internal Audit

INTERNAL AUDIT CHARTER

Purpose and Mission

The purpose of the City of Brampton's ("City") Office of Internal Audit ("Internal Audit") is to provide independent, objective assurance and consulting services designed to add value and improve the operations of the City. The mission of Internal Audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight. Internal Audit helps the City accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

Definitions

Audit Committee:	A Committee of Council. The Committee was established to enable members of Council to further enhance oversight capabilities and stewardship responsibilities. Roles and Responsibilities are further defined in the Audit Committee Terms of Reference.
Chief Audit Executive:	The Director of the Office of Internal Audit.
City Related Boards:	Includes Brampton Heritage Board and Brampton Library.
Consulting Services	Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve the City's governance, risk management, and control processes without the CAE and/or the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation and training.
Council:	Municipal Council of the City of Brampton and includes the Mayor and Councillors.
Employee:	An individual employed by the City, including those employed on contract and volunteers, but does not include those retained by the City on a professional services agreement.
Engagement:	A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review,

	fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives. An engagement includes financial, operational, compliance, follow up, information systems audits, other special audits, or consulting services.
Internal Audit Work Plan:	The plan approved by Council listing all engagements to be performed by Internal Audit.

Standards for the Professional Practice of Internal Audit

Internal Audit will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' ("the IIA") International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing,* and the Definition of Internal Auditing. The IIA's Mandatory Guidance constitutes the fundamental requirements for the professional practice of internal auditing and the principles against which to evaluate the effectiveness of internal audit activity's performance. The Chief Audit Executive ("CAE") will report periodically to the Audit Committee regarding Internal Audit's conformance to the Code of Ethics and the *Standards*. In addition, Internal Audit will adhere to and ensure conformance to the guidelines and procedures of ISACA for any engagements involving information systems.

Internal Audit will adhere to the City's relevant policies and procedures.

Authority

The CAE will report functionally to the Audit Committee and administratively (i.e. day-to-day operations) to the Chief Administrative Officer ("CAO"). To establish, maintain, and assure that the City's Internal Audit has sufficient authority to fulfill its duties, the Audit Committee will:

- Approve the Internal Audit Charter.
- Approve the risk-based Internal Audit Work Plan.
- Approve Internal Audit's budget and resource plan.
- Receive communications from the CAE on Internal Audit's performance relative to its plan and other matters.
- Approve decisions regarding the appointment and removal of the CAE.
- Review and approve, together with the CAO, the performance of the CAE.
- Approve decisions relating to the remuneration of the CAE.
- Make appropriate inquiries of management and the CAE to determine whether there is inappropriate scope or resource limitations.

The CAE will have unrestricted access to, and communicate and interact directly with, the Audit Committee, including private meetings without management present.

The Audit Committee authorizes Internal Audit to:

- Have full, free, and unrestricted access to all functions, records, properties, and personnel necessary to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information, and applicable law.
- Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- Obtain assistance from the necessary personnel of the City, as well as other specialized services from within or outside the City, in order to complete the engagement.
- Conduct any engagement of all City departments and special interest groups, 3rd parties (via right to audit clauses where applicable) and City Related Boards.

It is the duty of any employee of the City or City Related Board having control of records to permit the CAE or his/her designate access and examination when requested subject to applicable law. It is also the duty of any employee of the City or City related Board to fully co-operate with and make full disclosure of all pertinent information to the CAE or his/her authorized designate.

Independence and Objectivity

The CAE will ensure that Internal Audit remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the CAE determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to appropriate parties.

Internal auditors will maintain an impartial, unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing any operational duties for the City or City Related Boards.
- Initiating or approving transactions external to Internal Audit.
- Directing the activities of any City employee not employed by Internal Audit, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

The CAE will have no direct operational responsibility or authority over any operational activity for the City or City Related Boards. The CAE is not authorized to perform any operational duties for the City or City Related Boards.

Internal auditors will:

- Disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties.
- Exhibit professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.
- Make balanced assessments of all available and relevant facts and circumstances.
- Take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgements.

The CAE will confirm to the Audit Committee, at least annually, the organizational independence of Internal Audit.

The CAE will disclose to the Audit Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

Scope of Internal Audit Activities

The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the Audit Committee on the adequacy and effectiveness of governance, risk management, and control processes for the City. Internal Audit assessments include evaluating whether:

- Risks relating to the achievement of the City’s strategic objectives are appropriately identified and managed.
- The actions of the City’s officers, directors, employees, and contractors are in compliance with the City’s policies, procedures, and applicable laws, regulations, and governance standards.
- The results of operations or programs are consistent with established goals and objectives
- Operations or programs are being carried out effectively and efficiently.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the City.
- Information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity.
- Resources and assets are acquired economically, used efficiently, and protected adequately.

The CAE will report periodically to the Audit Committee regarding:

- The Internal Audit Charter.
- The independence of the Internal Audit activity.
- The Internal Audit Work Plan and progress against the plan.
- Internal Audit resource requirements.
- Results of Internal Audit activities, including significant risk exposures and control issues.
- Conformance with the IIA Code of Ethics and the *Standards*, and any action plans that address any significant conformance issues.
- Management's response to risk that, in the CAE's judgement, may be unacceptable to the City.

The CAE shares information, coordinates activities, and considers relying on the work of other internal and external assurance and consulting service providers as needed to ensure proper coverage and minimize duplication of efforts. Internal Audit may perform advisory and related client service activities, the nature and scope of which will be agreed with the client, provided Internal Audit does not assume management responsibility.

Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

Responsibility

The CAE has the responsibility to:

- Submit, at least annually, to the Audit Committee, a risk-based Internal Audit Work Plan for review and approval. The Internal Audit Work Plan sets out the priorities for Internal Audit that: are reflective of the City's objectives, concerns and priorities; are integrated and coordinated with the corporate risk assessment and strategic planning process: and, considers input from senior management.
- Communicate to the Audit Committee the impact of resource limitations on the Internal Audit Work Plan.
- Review and adjust the Internal Audit Work Plan, as necessary, in response to changes in the City's business, risks, operations, programs, systems, and controls.
- Communicate to the Audit Committee any significant interim changes to the Internal Audit Work Plan.
- Ensure each engagement of the Internal Audit Work Plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.

- Follow up on engagement findings and corrective actions, and report periodically to the Audit Committee any corrective actions not effectively implemented.
- Manage and coordinate all fraud investigation activities within City Departments and Related Boards.
- Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
- Ensure Internal Audit collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the Internal Audit Charter.
- Ensure emerging trends and successful practices in internal auditing are considered.
- Establish and ensure adherence to policies and procedures designed to guide Internal Audit.
- Ensure adherence to the City's relevant policies and procedures, unless such policies and procedures conflict with the Internal Audit Charter. Any such conflicts will be resolved or otherwise communicated to the Audit Committee.
- Ensure conformance of Internal Audit with the *Standards*, with the following qualifications:
    - If Internal Audit is prohibited by law or regulation from conformance with certain parts of the *Standards*, the CAE will ensure appropriate disclosures and will ensure conformance with all other parts of the *Standards*.
    - If the *Standards* are used in conjunction with requirements issued by ISACA, the CAE will ensure that Internal Audit conforms with the *Standards*, even if Internal Audit also conforms with the more restrictive requirements of ISACA.

Quality Assurance and Improvement Program

Internal Audit will maintain a Quality Assurance and Improvement Program ("QAIP") that covers all aspects of Internal Audit. The program will include an evaluation of Internal Audit's conformance with the *Standards* and an evaluation of whether internal auditors apply the IIA's Code of Ethics. The program will also assess the efficiency and effectiveness of Internal Audit and identify opportunities for improvement.

The CAE will communicate to the Audit Committee on Internal Audit's QAIP, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the City.

FLOWER CITY
BRAMPTON.CA

Corporation of the City of Brampton
The Office of Internal Audit

INTERNAL AUDIT CHARTER

Purpose and Mission

The purpose of the City of Brampton's ("City") Office of Internal Audit ("Internal Audit") is to provide independent, objective assurance and consulting services designed to add value and improve the operations of the City. The mission of Internal Audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight. Internal Audit helps the City accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

Definitions

Audit Committee:	A Committee of Council. The Committee was established to enable members of Council to further enhance oversight capabilities and stewardship responsibilities. Roles and Responsibilities are further defined in the Audit Committee Terms of Reference.
Chief Audit Executive:	The Director of the Office of Internal Audit.
City Related Boards:	Includes Brampton Heritage Board and Brampton Library.
Consulting Services	Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve the City's governance, risk management, and control processes without the CAE and/or the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation and training.
Council:	Municipal Council of the City of Brampton and includes the Mayor and Councillors.
Employee:	An individual employed by the City, including those employed on contract and volunteers, but does not include those retained by the City on a professional services agreement.
Engagement:	A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may

	include multiple tasks or activities designed to accomplish a specific set of related objectives. An engagement includes financial, operational, compliance, follow up, information systems audits, other special audits, or consulting services.
Internal Audit Work Plan:	The plan approved by Council listing all engagements to be performed by Internal Audit.

Standards for the Professional Practice of Internal Audit

Internal Audit will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' ("the IIA") International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing,* and the Definition of Internal Auditing. The IIA's Mandatory Guidance constitutes the fundamental requirements for the professional practice of internal auditing and the principles against which to evaluate the effectiveness of internal audit activity's performance. The Chief Audit Executive ("CAE") will report periodically to the Audit Committee regarding Internal Audit's conformance to the Code of Ethics and the *Standards*. In addition, Internal Audit will adhere to and ensure conformance to the guidelines and procedures of ISACA for any engagements involving information systems.

Internal Audit will adhere to the City's relevant policies and procedures.

Authority

The CAE will report functionally to the Audit Committee and administratively (i.e. day-to-day operations) to the Chief Administrative Officer ("CAO"). To establish, maintain, and assure that the City's Internal Audit has sufficient authority to fulfill its duties, the Audit Committee will:

- Approve the Internal Audit Charter.
- Approve the risk-based Internal Audit Work Plan.
- Approve Internal Audit's budget and resource plan.
- Receive communications from the CAE on Internal Audit's performance relative to its plan and other matters.
- Approve decisions regarding the appointment and removal of the CAE.
- Review and approve, together with the CAO, the performance of the CAE.
- Approve decisions relating to the remuneration of the CAE.
- Make appropriate inquiries of management and the CAE to determine whether there is inappropriate scope or resource limitations.

The CAE will have unrestricted access to, and communicate and interact directly with, the Audit Committee, including private meetings without management present.

The Audit Committee authorizes Internal Audit to:

- Have full, free, and unrestricted access to all functions, records, properties, and personnel necessary to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information, and applicable law.
- Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- Obtain assistance from the necessary personnel of the City, as well as other specialized services from within or outside the City, in order to complete the engagement.
- Conduct any engagement of all City departments and special interest groups, 3rd parties (via right to audit clauses where applicable) and City Related Boards.

It is the duty of any employee of the City or City Related Board having control of records to permit the CAE or his/her designate access and examination when requested subject to applicable law. It is also the duty of any employee of the City or City related Board to fully co-operate with and make full disclosure of all pertinent information to the CAE or his/her authorized designate.

Independence and Objectivity

The CAE will ensure that Internal Audit remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the CAE determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to appropriate parties.

Internal auditors will maintain an impartial, unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing any operational duties for the City or City Related Boards.
- Initiating or approving transactions external to Internal Audit.
- Directing the activities of any City employee not employed by Internal Audit, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

The CAE will have no direct operational responsibility or authority over any operational activity for the City or City Related Boards. The CAE is not authorized to perform any operational duties for the City or City Related Boards.

Internal auditors will:

- Disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties.
- Exhibit professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.
- Make balanced assessments of all available and relevant facts and circumstances.
- Take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgements.

The CAE will confirm to the Audit Committee, at least annually, the organizational independence of Internal Audit.

The CAE will disclose to the Audit Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

Scope of Internal Audit Activities

The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the Audit Committee on the adequacy and effectiveness of governance, risk management, and control processes for the City. Internal Audit assessments include evaluating whether:

- Risks relating to the achievement of the City’s strategic objectives are appropriately identified and managed.
- The actions of the City’s officers, directors, employees, and contractors are in compliance with the City’s policies, procedures, and applicable laws, regulations, and governance standards.
- The results of operations or programs are consistent with established goals and objectives
- Operations or programs are being carried out effectively and efficiently.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the City.
- Information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity.
- Resources and assets are acquired economically, used efficiently, and protected adequately.

The CAE will report periodically to the Audit Committee regarding:

- The Internal Audit Charter.
- The independence of the Internal Audit activity.
- The Internal Audit Work Plan and progress against the plan.
- Internal Audit resource requirements.
- Results of Internal Audit activities, including significant risk exposures and control issues.
- Conformance with the IIA Code of Ethics and the *Standards*, and any action plans that address any significant conformance issues.
- Management's response to risk that, in the CAE's judgement, may be unacceptable to the City.

The CAE shares information, coordinates activities, and considers relying on the work of other internal and external assurance and consulting service providers as needed to ensure proper coverage and minimize duplication of efforts. Internal Audit may perform advisory and related client service activities, the nature and scope of which will be agreed with the client, provided Internal Audit does not assume management responsibility.

Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

Responsibility

The CAE has the responsibility to:

- Submit, at least annually, to the Audit Committee, a risk-based Internal Audit Work Plan for review and approval. The Internal Audit Work Plan sets out the priorities for Internal Audit that: are reflective of the City's objectives, concerns and priorities; are integrated and coordinated with the corporate risk assessment and strategic planning process: and, considers input from senior management.
- Communicate to the Audit Committee the impact of resource limitations on the Internal Audit Work Plan.
- Review and adjust the Internal Audit Work Plan, as necessary, in response to changes in the City's business, risks, operations, programs, systems, and controls.
- Communicate to the Audit Committee any significant interim changes to the Internal Audit Work Plan.
- Ensure each engagement of the Internal Audit Work Plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
- Follow up on engagement findings and corrective actions, and report periodically to the Audit Committee any corrective actions not effectively implemented.

- Manage and coordinate all fraud investigation activities within City Departments and Related Boards.
- Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
- Ensure Internal Audit collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the Internal Audit Charter.
- Ensure emerging trends and successful practices in internal auditing are considered.
- Establish and ensure adherence to policies and procedures designed to guide Internal Audit.
- Ensure adherence to the City's relevant policies and procedures, unless such policies and procedures conflict with the Internal Audit Charter. Any such conflicts will be resolved or otherwise communicated to the Audit Committee.
- Ensure conformance of Internal Audit with the *Standards*, with the following qualifications:
    - If Internal Audit is prohibited by law or regulation from conformance with certain parts of the *Standards*, the CAE will ensure appropriate disclosures and will ensure conformance with all other parts of the *Standards*.
    - If the *Standards* are used in conjunction with requirements issued by ISACA, the CAE will ensure that Internal Audit conforms with the *Standards*, even if Internal Audit also conforms with the more restrictive requirements of ISACA.

Quality Assurance and Improvement Program

Internal Audit will maintain a Quality Assurance and Improvement Program ("QAIP") that covers all aspects of Internal Audit. The program will include an evaluation of Internal Audit's conformance with the *Standards* and an evaluation of whether internal auditors apply the IIA's Code of Ethics. The program will also assess the efficiency and effectiveness of Internal Audit and identify opportunities for improvement.

The CAE will communicate to the Audit Committee on Internal Audit's QAIP, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the City.

Appendix 3

AUDIT COMMITTEE
Terms of Reference

Composition:
- Minimum of five members of Council
- The Mayor, who is an *ex-officio* member
- Minimum of one to a maximum of three citizen members

Term of Office: Concurrent with the term of Council, ending November 30, 2022, or until successors are appointed

Established by: Council Resolution

Meetings: Quarterly, or as required by the Chair

Reports to: City Council

Supported by: City Clerk's Office

Qualifications:

Elected Officials:
- Where feasible, a background in finance, audit, or accounting would provide the Committee with additional expertise

Citizen Member(s):
- Lives and/or operates a business in Brampton
- Has a professional Accounting designation with a minimum of 10 years experience
- Demonstrates skill in strategy and innovation
- Proficient in accounting and auditing
- Displays exceptional verbal, written, listening, teamwork and collaboration skills

Objectives of the Audit Committee:

The objective of the Audit Committee is to enhance Council's understanding of financial and control reporting both internally (as provided by the City's Internal Audit Division) and statutorily (as provided by the City's Auditors). The Committee enables Council to fulfill its oversight and stewardship responsibilities. The Committee also provides a focal point for improved communication between Council, the Internal and Statutory Auditors, and Management. The Committee strengthens the impartial, objective and independent review of management practices through the internal and statutory audit functions. In particular, the Committee's objectives are to:

- Demonstrate a higher level of public accountability;
- Provide additional assurance to the public that City services are administered in an effective, efficient and economical manner;
- Ensure compliance with legislation for public reporting;
- Ensure compliance with Corporate policies and procedures;
- Ensure the safeguarding of City assets; and
- Ensure impartial, objective and independent review of processes for City operations

Responsibilities of the Audit Committee

The Audit Committee is responsible for:

Statutory Audit Function

Making recommendations to City Council regarding the following:

- The selection and dismissal of the City's statutory Auditor(s) in accordance with the requirements of Section 296 of the *Municipal Act, 2001*;
- The terms of engagement, fees and scope of the audit services provided;
- The review and approval of the annual Audited Financial Statements; and
- The review and receipt of reports.

Internal Audit Function

- Reviewing and approving the risk based internal audit work plan as recommended by the Chief Audit Executive ("CAE");
- Reviewing and approving the Internal Audit Charter;
- Reviewing Internal Audit reports issued during the year;
- Reviewing adequacy of the management responses to audit concerns in relation to the risks and costs involved;
- Ensuring the Internal Audit recommendations are implemented by reviewing Internal Audit's follow up reports;
- Reviewing and approving the Office of Internal Audit's budget;
- Approving decisions regarding the appointment and removal of the CAE;
- Reviewing the adequacy of the authority, responsibilities and functions of the City's Office of Internal Audit, including Internal Audit plans, budget, and the scope and results of internal audits and management's responses thereto;
- Ensuring all Internal Audit activities are free from interference and related implications;
- Reviewing with the CAE the performance of the Internal Audit function;
- Reviewing and approving, together with the CAO, the performance of the CAE; and
- Reviewing and approving decisions relating to the remuneration of the CAE.

Financial and Other Reporting

- Reviewing the annual Management Letter prepared by the City's statutorily appointed auditors and the related management responses.

General

- Reviewing the Audit Committee mandate periodically;
- Communicating and meeting independently with the CAE as appropriate; and
- Any other matters that could come within the scope of the auditors.

Report

Audit Committee

The Corporation of the City of Brampton

March 19, 2019

Date: January 2, 2019

Subject: **Internal Quality Assessment Review Results**

Contact: Foruzan Velji, Director, Office of Internal Audit, Office of the Chief Administrative Officer, 905-874-2215, Foruzan.Velji@brampton.ca

Recommendations:

1. That the report from Foruzan Velji, Director, Office of Internal Audit, dated January 2, 2019, to the Audit Committee Meeting of March 19, 2019, re: **Internal Quality Assessment Review Results**, be received.

Overview:

- The Office of Internal Audit performs an internal assessment (IQA) of its processes on an annual basis in accordance with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing ("*Standards*").
- The IQA's for 2016 and 2017 were not completed in a timely manner. This had been noted in the External Quality Assessment (EQA) performed in 2017. The IQA for 2018 was completed in a timely manner, at the end of the 2018 calendar year.
- The IQA results demonstrate that the work to enhance the internal audit methodology and best practices planned and undertaken by the Director, Office of Internal Audit has resulted in a significant improvement towards full conformance with the *Standards* with only minor improvement identified in the 2018 IQA. The IQA confirms that the Office of Internal Audit conforms to the IIA Code of Ethics.
- An external assessment ("EQA") of the Office of Internal Audit was completed in May 2017 by Protiviti and the results presented to Audit Committee at the June 12, 2017 meeting. A new EQA will be planned in the near future to provide independent assurance that the Office of Internal Audit is performing its work in conformance with the *Standards*.

Background:

The Office of Internal Audit has been working towards achieving conformance with the *Standards*[1] for the last two years. The External Quality Assessment by Protiviti in May 2017 identified several areas where practices within the Office of Internal Audit needed to be revised and brought up to standard.

The *Standards* require that the Chief Audit Executive, i.e. the Director, Office of Internal Audit, develops and maintains a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit activity. The QAIP must include both internal and an external assessments ("EQA"). The internal assessments ("IQA") must include ongoing monitoring of the performance of the internal audit activity, which is achieved by a quality assessment ("file QA") of each audit engagement after the audit report has been presented to Audit committee. This file QA checks for conformance to the *Standards,* and the Code of Ethics for internal auditors across such areas as planning, audit evidence, reporting, monitoring, and file completion. Any non-conformance items are discussed with the audit team and, if necessary, solutions are implemented to ensure the non-conformance does not repeat. The IQA also includes periodic self-assessments of the internal audit practices covering all areas of the department.

The ongoing IQA's focus on continuous improvement of the internal audit activity and involve monitoring its efficiency and effectiveness.

The *Standards* require that an EQA is done at least once every five years by a qualified, independent assessor or assessment team from outside the organization.

The results of both the internal and external assessments must be discussed with the Audit Committee as stated in the *Standards*.

Current Situation:

Internal Assessments

The 2016 and 2017 IQA's were not completed in a timely manner. With the hiring of the Director, Office of Internal Audit in December 2016, the function has started to be brought back into conformance with the Standards.

To compensate for the lack of timely IQA's, the Director, Office of Internal Audit, procured an EQA, which was performed by Protiviti in May 2017 and the results were reported to the Audit Committee at the June 12, 2017 meeting.

The 2018 assessment has been completed in a timely manner based on defined internal standards.

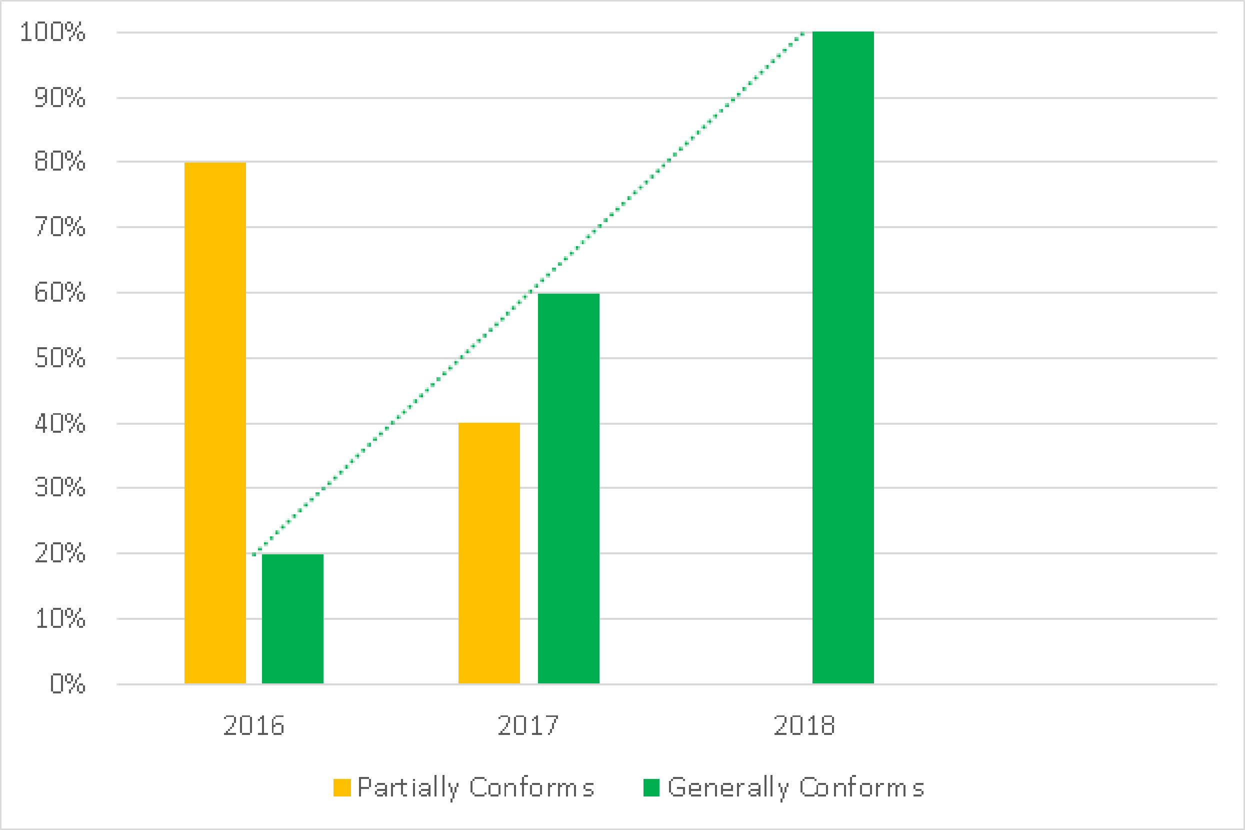
The results for 2016, 2017, and 2018 IQA's show the two year path towards full conformance with the *Standards* achieved in 2018. The IQA's also confirm that the eight gaps identified by the

---

[1] The conformance is to both the Standards and the IIA's Code of Conduct. The use of the word *Standards* includes both.

EQA in 2017 have been closed. Details of all (both IQA and EQA) gaps are summarized in Table 1. The only improvement opportunity noted in the IQA for 2018 was that documentation was lacking in two files regarding the sample size methodology used. It must be noted that the work performed conformed with the Office of Internal Audit sample size methodology and appropriate sampling was performed.

Table 1 – Three Year Trend of Conformance with IIA Professional Standards



The criteria used to determine conformance with the *Standards* are from the IIA itself and are as follows[2]:

Generally Conforms: The relevant structures, policies, and procedures of Internal Audit as well as the processes by which they are applied, comply with the requirements of the *Standard* or element of the (IIA) Code of Ethics in all material respects. There may be significant opportunities for improvement, but these must not represent situations where the activity has not implemented the *Standard* or the Code of Ethics, has not applied them effectively, or has not achieved their stated objectives.

---

[2] The wording of the criteria is exactly as stated in the IIA Guidance material on Quality Assessments.

5.2-4

Partially Conforms:	The activity is making good-faith efforts to comply with the requirements of the *Standard* or element of the (IIA) Code of Ethics and/or achieving their objectives.
Does not Conform:	The activity is not aware of, is not making a good-faith effort to comply with, or is failing to achieve many/all of the objectives of the *Standard* or element of the (IIA) Code of Ethics. These deficiencies will usually have a significant negative impact on Internal Audit's effectiveness.

The improvements made in the Internal Audit practices to achieve full compliance are detailed in Table 2.

Table 2: EQA/IQA issue Resolution

Issue	EQA Gap?	IQA Year	Addressed	Work done
Charter is not aligned with practices required per the *Standards*. **Audit committee Terms of Reference not fully aligned**	1 and 2	2016	2017 2018	Charter Revisions Charter reviewed per IIA *Standards* requirement Audit Committee Terms of Reference Updated
Department lacks a qualified IT auditor	3	2016, 2017	2018	Qualified IT Senior Advisor hired April 2018
Policies and procedures for the conduct of the IA function not reviewed, nor updated to reflect *Standards*		2016, 2017	2018	Internal Reference Manual reviewed and updated
IQA not performed in a timely manner or at all **2015 and 2016 Internal Audit Plans not completed in a timely manner** **One audit in 2016 was significantly delayed**	4, 5 and 6	2016, 2017	2017, 2018	Good faith efforts made in 2017 to complete all outstanding 2016 audits and file QA reviews. Work was caught up in mid 2018 on file QA's. In 2018 all file QA's are scheduled and assigned; a review time frame is established; and the 2016, 2017, and 2018 overall IQA's are completed

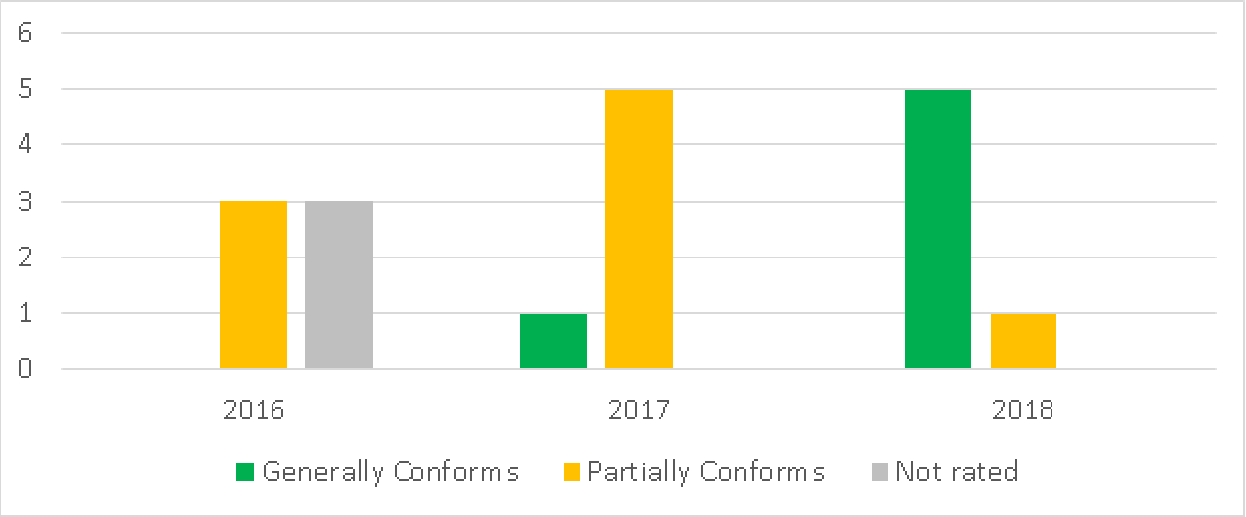
5.2-5

Issue	EQA Gap?	IQA Year	Addressed	Work done
Documentation standards are poor and inconsistent (EQA noted that a formal process to track time budgets vs. actual was missing)	8	2016	2017	The creation of a standardized file structure and templates are created to ensure work is documented in a consistent and appropriate manner Time budgets were implemented in 2017
Minor documentation issues – mostly around documenting audit objectives and scope and discussions within IA team		2017	2018	Templates and file structure reviewed for concordance and amended where needed.
Very minor documentation issue: two instances noted where information about testing (population and sample selection) were not documented but testing was performed appropriately		2018	2018	Audit Data Analytics template created

The remaining EQA gap (#7) was the fact that the last EQA was performed in 2011 which was six years prior to the EQA in 2017. The IIA Standards require an EQA to be performed every five years. This gap does not exist at this point in time. A new EQA is anticipated to be performed in the next year.

The IQA's also assess the Office of Internal Audit function against best practices in internal auditing. The results of this assessment shows the same trend. Six areas of best practices are assessed (in 2016 only 3 areas were assessed).

Table 3 – Three Year Trend of Conformance with Best Practices



The six best practices identified are:

- Signed engagement letters with clients to ensure the work to be undertaken through the audit is clear and agreed to by all parties.
- The outcome of important meetings during the planning process are documented in the file using a consistent format.
- The use of time budgets to assess efficiency.
- A mandated sample size methodology to be used on all audits.
- Filing and storing of both the electronic and hard copy working papers in accordance with mandated working paper documentation standard and the retention policy.
- A feedback survey is sent out after the completion of each audit to gauge auditee satisfaction with the audit process to ensure the division continues to improve its practices where required.

Corporate Implications:

Financial Implications:

None

Other Implications:

The City of Brampton has an independent Internal Audit function which provides the Audit Committee with objective assurance that the City is being managed in an efficient and effective manner, is managing risks appropriately, has appropriate governance structures in place, is safeguarding the assets of the City appropriately and is complying with applicable laws and regulations. It is important the Office of Internal Audit conducts itself in conformance with internally recognized professional standards to provide the Audit Committee with the assurance that work performed and items reported to the Audit Committee can be relied upon.

Strategic Plan:

This report achieves the Strategic Plan priority of Good Government through the objective and independent assurance that the operations of the City of Brampton are being assessed by a team of professional internal auditors who adhere to an internally recognized framework of auditing standards and code of ethics.

Conclusion:

The results of the IQA's provides the Audit Committee with the assurance that the Office of Internal Audit conducts its work in accordance with the audit profession's internationally recognized framework of standards and ethics. The Audit Committee can rely on the work performed by the Office of Internal Audit and on the results of the work presented to Audit Committee through various reports. The Office of Internal Audit has worked hard under the auspices of the Director, Office of Internal Audit, to conform to the Standards to provide the Audit Committee with the assurance that Office of Internal Audit's independent and objective assessment of management's ability to conduct the affairs of the City of Brampton through good governance.

Approved by:

Foruzan Velji, CPA, CA, CIA, CISA
Director, Internal Audit

Report authored by: Ella Kila, CPA, CA, CRMA
Senior Advisor, Internal Audit

BRAMPTON
Flower City
brampton.ca

Report
Audit Committee
The Corporation of the City of Brampton
March 19, 2019

Date: February 7, 2019

Subject: **Status of Management Action Plans-December 31, 2018**

Contact: Foruzan Velji, Director, Office of Internal Audit, 905-874-2215, foruzan.velji@brampton.ca

Recommendations:

That the report from Foruzan Velji, Director, Office of Internal Audit, dated February 7, 2019 to the Audit Committee Meeting of March 19, 2019, re: **Status of Management Action Plans – December 31, 2018** be received.

Overview:

- As part of the internal audit follow-up process, departments are required to provide the Office of Internal Audit with an update on the Management Action Plan status and progress of outstanding audit recommendations;
- The objective of this report is for the Office of Internal Audit to inform Audit Committee members on the progress of the implementation of recommendations, as reported by management;
- The comments reflect the status of the implementation of recommendations due to be completed by or prior to December 31, 2018;
- Since September 2018, 36 audit recommendations were to be implemented by management; a total of 10 recommendations were implemented, of which 2 were proactively completed, and 26 have been deferred.
- The Office of Internal Audit may validate results at a subsequent date as part of the follow-up audit process;
- Details concerning the individual recommendations are available upon request.

Background:

In accordance with the requirements of Standard 2500.A1 of the International Standards for the Professional Practice of Internal Auditing, the Office of Internal Audit has established a follow-up process to monitor and ensure that management action plans for audit recommendations have been implemented. This process has been in place since 2006.

For the follow-up process, departments are required to provide an update to the Office of Internal Audit on the progress of implementing agreed-upon audit recommendations. The Office of Internal Audit reviews the comments submitted by the department, and where necessary, the Director of Internal Audit will meet with Management to discuss the respective progress and comments. Upon complete implementation of the audit recommendations by Management, Internal Audit will assess whether a follow-up audit is necessary to validate that the implemented processes and procedures are operating effectively. Such follow-up audits are included in Internal Audit's annual work plan, which is approved by the Audit Committee.

The implementation status updates from Management are reported to the Audit Committee. This report summarizes the statuses of audit recommendations due to be implemented by management on or prior to December 31, 2018.

Current Situation:

As of December 31, 2018, there were 36 audit recommendations that were due to be implemented by management on or prior to this date. 10 were reported as complete by management, and 26 have been deferred. 25 will be completed over the next year.

Please refer to **Appendix 1** for the details of the Recommendations as of December 31, 2018.

Corporate Implications:

Financial Implications:

None

Other Implications:

None

Strategic Plan:

This report achieves the Strategic Plan priority of Good Government through the establishment of an internal audit follow up procedure for the implementation of audit recommendations, which promotes corporate accountability, values, and governance best practice.

Conclusion:

The Office of Internal Audit is committed to continuously collaborating with management in identifying, reviewing, improving, and updating policies, procedures, and processes on a regular basis, and enhancing efficiencies and process effectiveness.

The Office of Internal Audit encourages management and staff to continue striving to meet the target completion dates of audit recommendations.

Attachments:

Appendix 1: Audit Recommendations as of December 31, 2018.

Foruzan Velji
Director & Chief Audit Executive, Office of Internal Audit

Report authored by: Sabrina Cook, Coordinator, Research & Administrative Services, Office of Internal Audit

Appendix 1: Audit Recommendations as of December 31, 2018

Audit Report	Rating	Year	Recs	Total Completed	As of December 31, 2018		
					Completed	Deferred	Not Yet Due
Transit: PRESTO Revenue	N/A	2016	7	5	-	-	2
Property Tax Revenue	🟩	2017	5	4	1	-	-
Human Resources Salary Administration	🟧	2017	13	12	-	1	-
Cash Handling and Revenue-Cassie Campbell Community Centre	🟩	2017	8	5	-	-	3
Employee Expense Reimbursement	🟨	2017	6	2	4	-	-
Library Operations	🟩	2017	4	4	-	-	-
Building Permits	🟨	2017	3	2	-	-	1
Mayor and Councillor Expenses	N/A	2017	7	7	-	-	-
Review of Logical Access Management	N/A	2018	6	-	-	6	-
Building Inspections	🟨	2018	4	-	-	2	2
By-Law Enforcement/Parking Infractions	🟨	2018	13	1	-	8	4
Fire and Emergency Services	🟨	2018	14	5	1	-	8
Corporate Security	🟥	2018	14	4	3	2	5
Road Resurfacing	🟨	2018	15	7	1	7	-
		TOTAL	**119**	**58**	**10**	**26**	**25**

BRAMPTON
brampton.ca Flower City

Report
Audit Committee
The Corporation of the City of Brampton
March 19, 2019

Date: January 7, 2019

Subject: **Corporate Fraud Prevention Hotline Update**

Contact: Foruzan Velji, Director, Office of Internal Audit, 905-874-2215, Foruzan.Velji@brampton.ca

Recommendations:

1. That the report from Foruzan Velji, Director, Office of Internal Audit, dated January 7, 2019, to the Audit Committee Meeting of March 19, 2019, re: **Corporate Fraud Prevention Hotline Update**, be received; and
2. That the Audit Committee endorse the continued operation of the Corporate Fraud Prevention Hotline.

Overview:

- The Corporate Fraud Prevention Hotline (Hotline) was launched on July 4, 2016 for the use of City of Brampton employees.
- The Hotline has received a total of 18 reports of alleged fraud. Since the last update to Audit Committee on June 26, 2018, three reports were received by the Hotline. Internal Audit conducted investigations of all 13 reports, three of which have been closed and 10 of which are open.
- There has been a 100% increase in the usage of the Hotline in 2018.
- Internal Audit will provide ongoing updates on the status of the Corporate Fraud Prevention Hotline to the Audit Committee.

Background:

As part of the City of Brampton's ("the City") commitment to protecting its assets, a framework to prevent, detect, and report incidents of fraud, as well as investigate any suspected acts of fraud was established. On July 4, 2016 the City launched Phase I of the Corporate Fraud Prevention Hotline, which allows City employees to report alleged incidents of fraud. The Hotline allows employees to report incidents anonymously and confidentially 24 hours a day, seven days a week. To report an incident of suspected fraud, employees can submit a report through the third party secure website or over the phone through a third party dedicated toll-free number.

Current Situation:

Internal Audit updates the Audit Committee on the status of the Hotline, including statistics on the number and types of reports received. From January 2018, the Hotline has received a total of 12 reports of alleged fraud. Since the update report was presented at the June 26, 2018 Audit Committee, the Hotline has received 3 new reports. Currently, there are 10 open reports, and investigations are being conducted by Internal Audit.

The following table provides a summary of all ongoing investigations between June 26, 2018 and Q4 2018:

New Reports Submitted as of June 2018			
Date Submitted	**Report Category**	**Report Method**	**Report Status**
September 2018	Embezzlement or Fraud	Web	Investigation complete
October 2018	Unethical conduct	Hotline	Investigation complete
November 2018	Non-compliance with Policy or Procedure	Web	Ongoing investigation
Other Investigations			
Date Submitted	**Report Category**	**Report Method**	**Report Status**
November 2017	Theft	Client transcribed	Closed
December 2017	Theft	Client transcribed	Investigation complete
March 2018	Embezzlement or Fraud	Web	Investigation complete
May 2018	Theft	Web	Investigation complete
May 2018	Violation of Laws, Regulations, Policies, Procedures	Hotline	Closed
May 2018	Theft	Client transcribed	Closed
May 2018	Theft	Client transcribed	Ongoing investigation
May 2018	Theft	Client transcribed	Ongoing investigation
May 2018	Theft	Client transcribed	Ongoing investigation
May 2018	Theft	Client transcribed	Ongoing investigation

Internal Audit performs its assurance and consulting activities guided by a philosophy of adding value to improve the operations of the City of Brampton. As part of this commitment, Internal Audit has updated the Fraud Prevention Hotline processes and procedures, created an awareness campaign of the Corporate Fraud Prevention Policy, and continues to encourage use of the Hotline, if required.

In 2018, there has been a 100% increase in the number of reports received through the Hotline. The increased usage supports the need for the City to have a dedicated third party Hotline.

Corporate Implications:

Financial Implications:

The 2018 operating budget approved by Council, includes amounts for implementation, maintenance, and operation of the Corporate Fraud Prevention Hotline.

Other Implications:

None

Strategic Plan:

This report achieves the Strategic Plan priority of Good Government through the support of the Corporate Fraud Prevention Policy and Hotline which promote corporate accountability, our corporate values and governance best practices.

Conclusion:

The Corporate Fraud Prevention Policy and Hotline enhances and strengthens the City's governance structure. It reinforces Council's expectations regarding rules of behavior and emphasizes the values of the City. The Office of Internal Audit will continue to update the Audit Committee on the status of the Hotline and any ongoing and/or completed fraud investigations.

Approved by:

Foruzan Velji, CPA, CA, CFI, CISA
Director, Office of Internal Audit

BRAMPTON
Flower City
brampton.ca

Report
Audit Committee
The Corporation of the City of Brampton
March 19, 2019

Date: February 5, 2019

Subject: **Internal Audit Work Plan – 2019**

Contact: Foruzan Velji, Director, Office of Internal Audit, 905-874-2215, Foruzan.Velji@brampton.ca

Recommendations:

1. That the report from Foruzan Velji, Director, Office of Internal Audit, dated February 5, 2019, to the Audit Committee Meeting of March 19, 2019, re: **Internal Audit Work Plan – 2019**, be received.

Overview:

- The 2019 Internal Audit work plan was developed using a risk-based approach which included input from senior management, issues from previous audits, evaluation of audit results and risk assessments.
- The objective of performing audits is to add value to improve the operations of the City as well as assist the City in accomplishing its objectives.
- On a regular basis, Internal Audit reviews and updates the work plan as needed based on current information, concerns and discussions with the leadership team, issues identified and risk reviews.
- This report provides Audit Committee with a status update of the Internal Audit Work Plan for 2018 as well as the Audit Work Plan for 2019.

Background:

The Internal Audit annual work plan was developed using a risk-based approach as outlined in the Internal Audit Charter. Several factors are taken into consideration in developing the Audit work plan such as:

- Risk assessment results;
- Last time the area/process was audited;

- Results of previous audits;
- Requests and information provided from Corporate Leadership Team or Senior Management.

Internal Audit is focused on performing an objective assessment of evidence to provide an independent opinion as to the effectiveness and efficiency of a process or system in order to assist departmental management in achieving their business objectives and goals.

The results of audits performed are communicated to the Audit Committee and the Corporate Leadership Team to provide information to assist them in carrying out their governance responsibilities.

Internal Audit also conducts consulting engagements at the request of management. Consulting services include advice, facilitation and training. For this activity, the nature and scope of the engagement are agreed upon between management and the Office of Internal Audit. The objective is for the Office of Internal Audit to add value and help improve an organization's risk management and control processes without assuming management responsibility. The results of consulting engagements are reported to departmental management.

The annual Audit work plan will be reviewed on a regular basis and may be adjusted based on any information, issues or concerns that have been identified. Updates and changes to the Audit work plan will be communicated to the Audit Committee.

Current Situation:

Appendix A reflects the status of the 2018 Audit work plan to date.

One audit, IT Disaster Recovery has been deferred to the 2019 Audit work plan, thereby changing the 2018 planned audits to ten. As of the date of this report, eight of ten audits have been completed. Two audits are currently underway with completion anticipated by April 2019.

The 2019 Audit work plan (**Appendix B**) sets out the priorities of the Internal Audit function that are reflective of the City of Brampton's strategic goals, objectives, concerns and priorities, integrated and coordinated with a corporate risk assessment. The annual Audit work plan is comprised of operational and compliance audits, investigations and follow up reviews. The Audit work plan was developed taking into consideration available Internal Audit staff resources.

Any changes to the Audit work plan may require the removal or deferral of a project identified within this report or alternatively, the hiring of an outside auditor to perform the audit. Any changes throughout the year will be communicated to the Audit Committee.

Internal Audit activities will be conducted in accordance with the International Standards for the Professional Practice of Internal Auditing. The specific scope of each project will be determined during the project planning phase.

Corporate Implications:

Financial Implications:

N/A

Other Implications:

N/A

Strategic Plan:

This report achieves the Strategic Plan priority of Good Government.

Conclusion:

The Internal Audit work plan will be reviewed on a regular basis and updated if needed. Our intention is to keep the Audit work plan agile and flexible, ensuring that identified risks are appropriately addressed. The Audit work plan is designed to add value to the organization and provide the highest standard of professional, independent and timely solutions in partnership with City departments.

Approved by:

Foruzan Velji, CPA, CA, CFI, CISA
Director, Office of Internal Audit

Attachments:

Appendix A: Update on Internal Audit Work Plan 2018

Appendix B: Internal Audit Work Plan 2019

Appendix A: Update on Internal Audit Work Plan 2018

Projects	Status
Mobile Phone Management Follow Up *To review the previously agreed upon recommendations to assess the efficiency and effectiveness of processes and the adequacy of internal controls.*	Completed 2018
Human Resources *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Recruitment - Completed 2018 Employee Benefits and Salary Administration – both in progress
IT Service Desk Management Audit (Phase 2) *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Completed 2018
Building Inspections Audit *To assess the adequacy and effectiveness of the building inspection processes, controls and compliance to policies, procedures, by-laws and legislation.*	Completed 2018
Construction Audit *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Completed 2018
Fire Services *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Completed 2018
Corporate Security *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Completed 2018
By law enforcement *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Completed 2018
IT Disaster Recovery *To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.*	Deferred to 2019
OTHER ITEMS: OFFICE OF INTERNAL AUDIT PROJECTS	
Electronic Audit Working Papers *To assess and review software alternatives for electronic audit working papers; if a suitable software is determined, to transition to electronic files.*	In progress
Fraud Prevention Hotline Review Part 2 *Update of policy and procedures including rollout of new materials to staff*	Completed 2018
Internal Audit Methodology Review Part 2 *Update of Internal audit division methodology including procedures manual update. Review of Audit committee overview manual.*	Completed 2018

Appendix B: Internal Audit Work Plan 2019

Projects

Transit Operations

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Human Resources – Employee Benefits (Phase 2)

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Rose Theatre Operations

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Contract Management

To assess the adequacy and effectiveness of the building inspection processes, controls and compliance to policies, procedures, by-laws and legislation.

Contract Cleaning

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Fleet

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Cash Handling and Revenue

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Payroll

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Accounts Payable

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Active Directory

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Fire Wall Rules

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Data Centre

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

IT Disaster Recovery

To assess effectiveness and efficiency of processes to determine adequacy of internal controls, compliance to policies, procedures and legislation.

Other Items: Office of Internal Audit Projects

Fraud Awareness Program

Creation and rollout of new materials to staff including March Fraud Prevention Month. Additional awareness activities and material to be delivered to staff throughout the year

Education and Outreach Program

Staff and community outreach events geared to provide information on the work contemplated by the Office of Internal Audit.

BRAMPTON
brampton.ca Flower City

Report
Audit Committee
The Corporation of the City of Brampton
March 19, 2019

Enhancement Required

Date: November 30, 2018

Subject: **IT Service Desk Audit Report**

Contact: Foruzan Velji, Director, Office of Internal Audit, 905-874-2215, foruzan.velji@brampton.ca

Executive Summary:

The IT Service Desk is provided by the Client Care Team in the Digital Innovation and IT Division (IT). The IT Service Desk is the primary point of contact for City of Brampton employees to report computer problems or to obtain IT services. In 2018, the IT Service Desk registered 33,175 tickets.

The IT Service Desk audit engagement was identified in the 2018 Audit Work Plan. The audit period covered October 1, 2017 to September 30, 2018.

Summary of Findings

There has been improvement in the IT Service Desk since it transitioned to IT from Service Brampton in December 2017. An IT Service Catalogue was deployed in May 2018 providing a continuum of new offerings on the Self-Service portal. This has resulted in an increasing usage of the Self-Service Portal.

User calls to the Service Desk will increase as the City of Brampton continues to see increasing data digitization and new systems that provide automation. Strengthening the IT Service Desk will help support City personnel as the use of information technology expands. While there are processes in place, enhancements are required by management:

- IT Service Desk processes are not followed consistently, out of hours issues are not recorded, and service level targets for low priority tickets are being breached;
- The process of root cause analysis is not fully developed; and,
- Guidelines for handling different types of tickets needs to be created; client care personnel process awareness and training needs improvement.

The nature of the above findings indicate a lack of management oversight. It should be noted that in December 2018 a Program Manager was hired to address these issues.

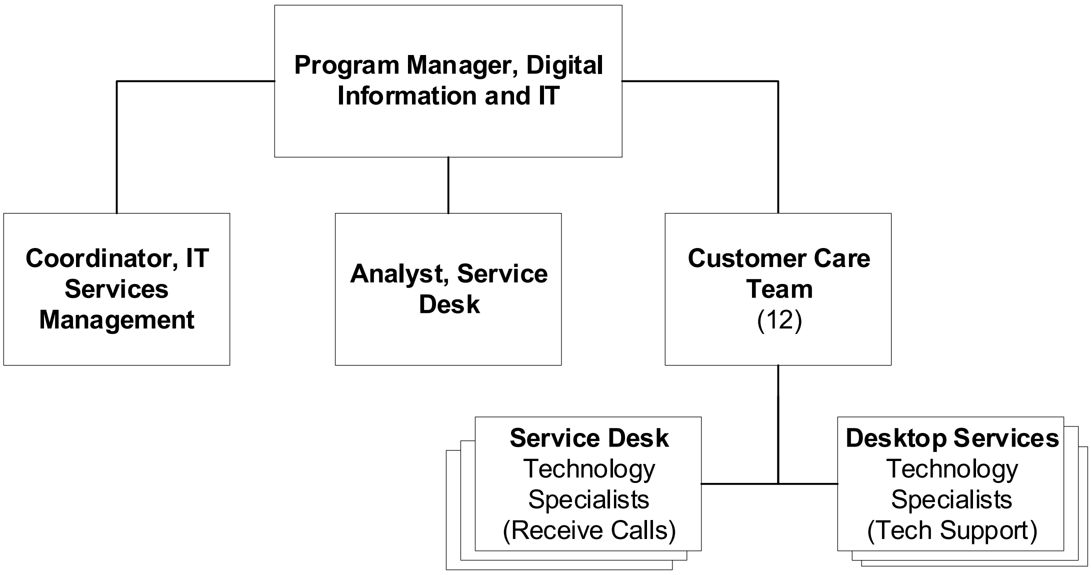
Background:

Client Care Team

The IT Service Desk (ITSD) function is provided by the Client Care team in the IT division. The ITSD serves as a single point of contact for the technology needs of approximately 6,000 City of Brampton employees.

There are currently 15 staff and management in the Client Care Team, providing day-to-day support including: Incident Management and Resolution, Change Management, Problem Management, Statistical Analysis and Technical Writing. The organizational chart is detailed in **Figure 1** below.

Figure 1: Organizational Chart - Client Care Team


Program Manager, Digital Information and IT
Coordinator, IT Services Management
Analyst, Service Desk
Customer Care Team
(12)
Service Desk
Technology Specialists
(Receive Calls)
Desktop Services
Technology Specialists
(Tech Support)

The Client Care Team provides Tier 1 and Tier 2 (see **Appendix C** for a description of tiered support structures) support for all applications and hardware for City of Brampton employees and Council via the telephone, electronic mail (email), a web based Self Service Portal, walk-in Service Centre, or on-site support. The team provides field support for over 100 locations around the City, including City Hall, the on-site Service Center, and the IT Service Desk by telephone. Tier 3 support is provided by specialist 'HEAT' teams outside of the Client Care Team.

As part of the Customer Care team, the Service Desk fields all incoming customer communications, and Desktop Services provides technical support. The Technology Specialists rotate between Service Desk and Desktop Services, and Tier 1 and Tier 2 tasks are shared amongst all members of the Customer Care Team.

ITSD Processes:

Hours of Support

The IT Service Desk phone queue is staffed by IT Technology Specialists from 8:30 am to 4:30 pm Monday through Friday. At 4:30 pm each weekday and on the weekends, the queue is automatically switched over to the Service Brampton Contact Centre where Customer Care Agents (CSAs) field the calls. The CSA creates tickets for callers and will perform Windows password resets, pin-pad resets and similar tasks after hours, from knowledge base articles that they follow. Most tickets are assigned to the Service Desk team for processing the next day.

Service Desk Tools

IT uses HEAT software by Ivanti for logging, assigning, and administering IT issues or requests received by the ITSD. For online services to City Employees, IT has implemented a web based Self-Service Portal using the self-service component of HEAT.

Recording Issues

ITSD logs issues into the HEAT system and IT Technology Specialists assign impact and urgency ratings. Email notification updates are automatically sent to employees.

Resolving Issues

Technology Specialists review the issues and perform the necessary work to resolve them, or the issues are escalated to Tier 3, one of the HEAT teams who have final responsibility to resolve issues.

Ticket Closure

The ticket status is set to 'Resolved/Fulfilled' by a team member after confirmation of resolution. The ticket is formally 'Closed' automatically by the tool 3 days after resolution.

ITSD Support

City employees who require IT support can contact the ITSD by telephone, email, the Self-Service Portal, or the walk-in Service Centre:

- Telephone: Employees can call 905-874-2029 to obtain immediate support for an issue. They also have the option of leaving a message. A Technology Specialist enters the information into HEAT, which generates a ticket and sends the employee a notification. Technology Specialists then work to resolve the issue, or reassign and escalate it to a HEAT team for resolution.
- Email: City employees can report issues via email (ITServiceDesk@brampton.ca). HEAT automatically generates a ticket and sends an email notification receipt to the employee. It is then resolved by a

Technology Specialist~~s~~, or reassigned and escalated to a HEAT team for resolution.

- Self-Service: The Self Service portal feature in HEAT allows employees to enter their own service requests and log issues. Employees are able to look up the status of their existing tickets and review answers to frequently asked IT questions. The employee is assigned an automated ticket and receives an email notification. Technology Specialists then work to resolve the issue, or reassign and escalate it to a HEAT team for resolution.

- Walk-Ins: Employees can physically walk to the second floor of West Tower for immediate assistance from IT. The issues are logged into HEAT and a ticket is assigned to a HEAT team unless the issue can immediately be resolved.

For the audit period, ITSD support by source was as follows:

Source	**Incidents**	**Service Requests**
Email	29.1%	0.1%
Phone	48.1%	16.2%
Self-Service	19.8%	64.5%
Walk-in	3.1%	0.6%
Converted from Incidents	N/A	18.7%

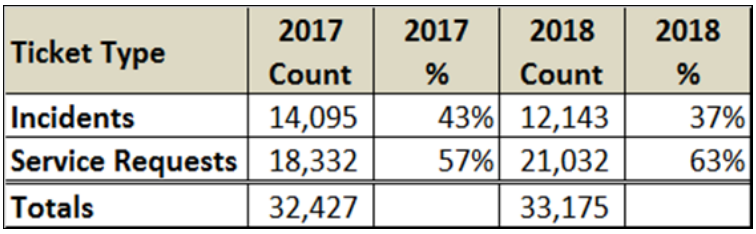
Service Desk Statistics – 2017-2018[1]

Every contact made to the Service Desk, whether by phone, email, Self-Service Portal or walk-in, generates an Incident or a Service Request ticket, which are defined as follows:

- An Incident is a computer related problem or IT service disruption that needs to be resolved; and,
- A Service Request is a user request not related to a service disruption, such as access to an IT service, IT information or advice, and standard and low cost hardware or software changes.

Additional tickets may be created when multiple tasks are assigned to resolve an issue. The table in **Figure 2** provides a combined count for each ticket type, by year.

Figure 2: Total Combined Incident and Service Desk Tickets, by Year



Ticket Type	2017 Count	2017 %	2018 Count	2018 %
Incidents	14,095	43%	12,143	37%
Service Requests	18,332	57%	21,032	63%
Totals	32,427		33,175	

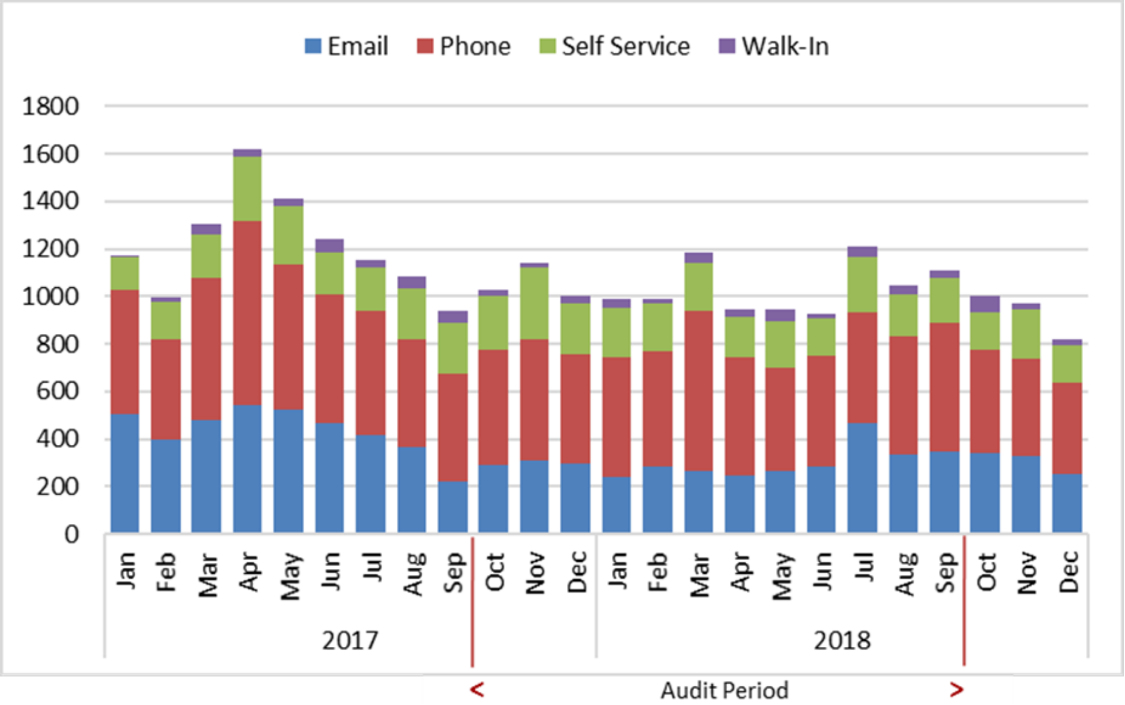
Figure 3 through to **Figure 6** further divide the counts into source categories. Source categories for both Incident and Service Requests includes email, telephone, self-service or walk-in.

Added Notes: Service Requests have an additional source category called ‘Converted from Incident’. Incidents that have been converted to Service Requests are included in the Service Desk count and are not duplicated. The source category ‘Voice Mail’ is common to both Incidents and Service Requests, and was merged into the source category ‘Phone’, as voice mail numbers are very small. The dates refer to the ticket creation date.

---

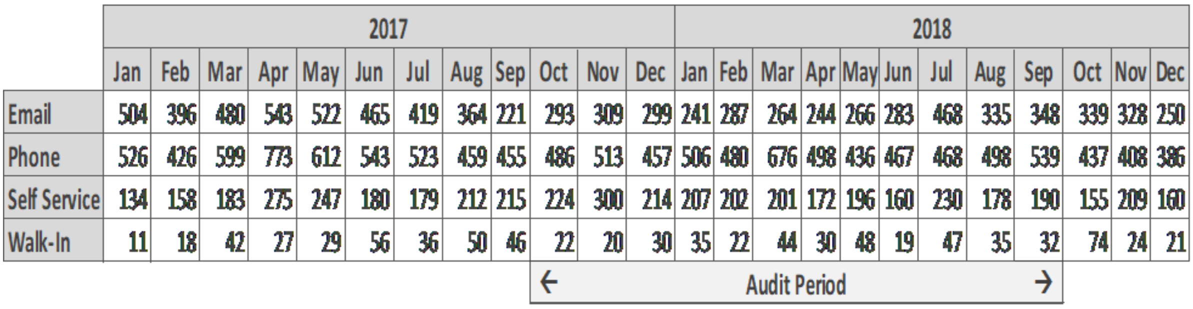
[1] The audit period ran from October 1, 2017 to September 30, 2018. Numbers from dates outside the audit period have not been audited.

Figure 3: Incidents by Source 2017 and 2018



Data outside the Audit Period has not been audited.

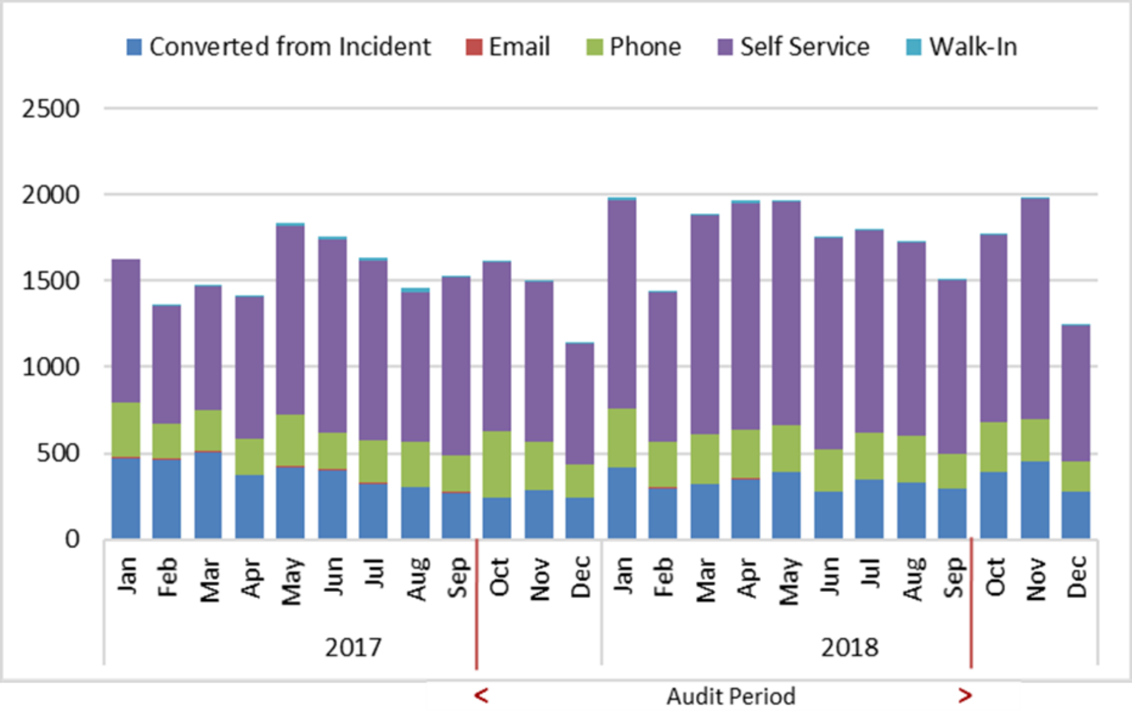
Figure 4: Incidents by Source 2017 and 2018



	2017												2018											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Email	504	396	480	543	522	465	419	364	221	293	309	299	241	287	264	244	266	283	468	335	348	339	328	250
Phone	526	426	599	773	612	543	523	459	455	486	513	457	506	480	676	498	436	467	468	498	539	437	408	386
Self Service	134	158	183	275	247	180	179	212	215	224	300	214	207	202	201	172	196	160	230	178	190	155	209	160
Walk-In	11	18	42	27	29	56	36	50	46	22	20	30	35	22	44	30	48	19	47	35	32	74	24	21

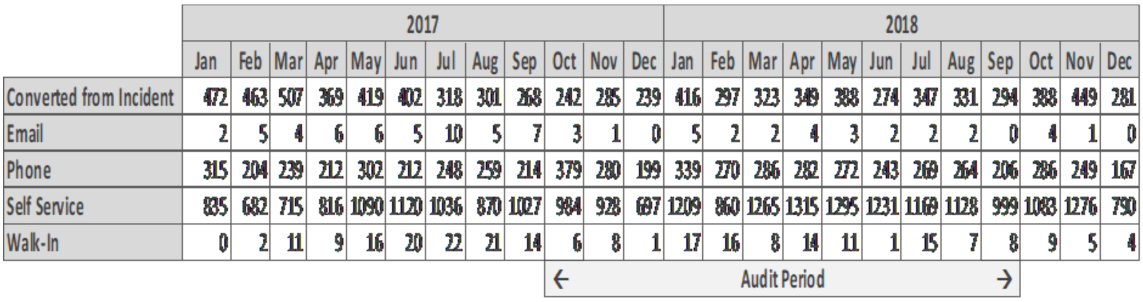
← Audit Period →

Figure 5: Service Requests by Source 2017 vs 2018



Data outside the Audit Period has not been audited.

Figure 6: Number of Service Requests by Source, 2017 vs 2018



	2017												2018											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Converted from Incident	472	463	507	369	419	402	318	301	268	242	285	239	416	297	323	349	388	274	347	331	294	388	449	281
Email	2	5	4	6	6	5	10	5	7	3	1	0	5	2	2	4	3	2	2	2	0	4	1	0
Phone	315	204	239	212	302	212	248	259	214	379	280	199	339	270	286	282	272	243	269	264	206	286	249	167
Self Service	835	682	715	816	1090	1120	1036	870	1027	984	928	697	1209	860	1265	1315	1295	1231	1169	1128	999	1083	1276	790
Walk-In	0	2	11	9	16	20	22	21	14	6	8	1	17	16	8	14	11	1	15	7	8	9	5	4

← Audit Period →

Audit Scope and Objectives:

Scope

The scope of the audit includes all IT Service Desk activities from October 1, 2017 to September 30, 2018.

Not be included in the scope of this audit were other service requests through 3-1-1 and Service Brampton.

Objective

The objective of this audit was to assess whether processes, procedures, and controls related to the IT Service Desk activities were adequately and appropriately designed and operating effectively.

Specifically, the following were assessed:

- Processes and controls around IT Service Desk issue and request intake, resolution, escalation and closure are adequately designed and operating effectively;
- Existing service level agreements, policies, standard operating procedures and guidelines are effective, sufficient and appropriate;
- Service Desk activity reports enable management to measure service performance and service response times, and to identify trends or recurring problems to support continuous improvement; and,
- IT Service Desk operations in relation to industry leading practices.

Findings and Recommendations:

KPMG was engaged to perform the audit. The sample size of 30,052 Service Desk tickets included Incidents and Service Requests and was restricted to the audit period October 1, 2017 to September 30, 2018. Appendix D of this report provides a table with the KPMG detailed findings, recommendations, and management responses. A summary of this Appendix is provided below.

The Service Desk Processes Are Not Followed Consistently Nor Are All Issues Recorded

P2

Process management and improvement are hampered when there is missing or incomplete information. There are a number of cases where policies and procedures are not being followed, including processes to proactively manage issues and to ensure all service levels are met. These factors increase the risk of service level breaches and extended service interruptions. Observations included:

- Out of hours system issues were not recorded in the HEAT ticketing system;
- 8.8% of the tickets were missing the mandatory category and/or priority fields;
- Not all contacts with the Service Desk were recorded, contrary to policy;
- The ticketing facility was not always used as designed;
- 7.2% of the low priority tickets breached service levels; and,
- The process in place to review and address weekly ticket reports was not followed consistently.

Summary of Management Responses including Timelines

A. Updates to the Incident Process are currently underway, including documentation and reporting. Management will enforce the process once documentation and training for Service Desk process participants is completed. Targeted completion end of March 2019.

B. A new or updated tool for incident management is being investigated that will include SLA integration. Targeted completion December 2019.

C. Queue Management practices and tools are being reviewed and changes will be rolled out in stages in 2019, including dashboards, the implementation of key performance indicators (KPI), and weekly metric reports and follow up. See the KPMG detailed findings table in Appendix D for specific timelines for each activity.

D. IT is investigating the ability to have ticket creation integrated with the infrastructure monitoring tools. Targeted completion December 2019.

2. Problem Management Is Not Fully Being Performed

P2

Problem Management identifies and addresses the root-cause of problems and analyzes trends over time. The current Problem Management practice is not a fully developed or mature process, which could lead to missed opportunities to prevent Incidents or mitigate their impact.

Management Response Including Timeline

A new process manager was hired as of December 2018 to explore these gaps and ensure management implements standard leading practices including and not limited to complete problem management. Process review, update and finalization will be completed by end of April 2019.

3. There Are No Explicit Policies For System Events and Request Management

P2

The lack of explicit guidelines on the differences in identifying and handling the different types of issues could lead to missing tickets or incorrect prioritization and resolution.

Process awareness and training can be improved. Without training staff on updates, new operational procedures may be inconsistently performed or not performed at all.

Management Response Including Timeline

A. The Incident Management process guide is currently being updated and improved. Targeted completion end of March 2019.

B. Service Request Management enhancement training will take place for those Queue Managers and staff that handle Service requests. Targeted for August 2019.

C. Integration of Service Request management software with the planned intake process (a separate initiative in IT) for all requests received by the division will help identify and categorize Service requests as project or operational. Projects will be further defined as capital budget request or current project change request. A manual process is in place currently that will be documented as a process by mid March 2019. System integration is targeted December 2019.

D. Periodical updates will start and be continuous as the Knowledge Articles mature. See Appendix D for detailed timelines.

E. Staff training is ongoing at monthly team meetings with Client Care staff, periodic updates are sent via email to staff regularity and stored on the client care site. See Appendix D for detailed timelines.

F. More formal rigor will be implemented in the following manner:
   - Knowledge Articles are updated and completed for all existing service offerings – target end of June 2019
   - Transition to Operations process is in place for net new services to include the creation of a Knowledge article and the subsequent training of Client Care staff to support – targeted end of June 2019

A new or updated tool for ITSM as a whole, which includes a detailed CMDB which is automated to search for a known error or Knowledge Article to assist Client Care staff as they create an incident, improving first point of contact resolution – targeted for end of December 2019

Conclusion:

With the increase in data digitization and new systems that provide automation, City employees will require more IT support.

Robust management oversight and effective management reporting will be sufficient to address the majority of the findings. A Program Manager was hired in December 2018. One of the roles of this manager will be to review the ITSD, ensuring consideration of best practices and customer service.

We thank the IT Service Desk team and management for their full cooperation and timely support during the audit.

Appendices:

Appendix A: Criteria for Audit Report Rating
Appendix B: Criteria for Evaluating Audit Findings
Appendix C: Three Tier Support Structure
Appendix D: Table of Findings, Recommendations, and Management Responses

Appendix A: Criteria for Audit Report Rating

The audit report rating is intended to provide management with an indication of the overall status of internal controls and processes in the audited area. The audit report rating is based on Internal Audit's overall assessment of the significance of issues identified during the audit process, and in conjunction with professional judgement also considers the following:

1. Design and effectiveness of internal controls, processes, procedures, policies, and systems.
2. Compliance with policies, standard operating procedures, and other requirements (i.e. legal, regulatory, accounting, contractual).
3. Quality of the data and information provided by management and related systems.
4. Efficiency of systems, processes and procedures.

Effective	- Key controls are adequately and appropriately designed, and are operating effectively to support objectives and manage risks. - Audit recommendations resulted in only minor enhancements to the effectiveness or efficiency of controls and processes. - One or more Priority 3 findings. - Insignificant cumulative financial impact when all audit findings have been considered. - Audit findings would not be subject to a follow-up by Internal Audit.
Enhancement Required	- A few key control weaknesses were noted that require enhancements to better support objectives and manage risks. - One Priority 2 finding and Priority 3 findings. - Priority 3 findings only where the cumulative financial impact is significant. - Corrective action and oversight by management is needed. - Audit findings could be subject to a follow-up by Internal Audit.
Significant Improvement Required	- Numerous key control weaknesses were noted that require significant improvement to support objectives and manage risks. - One Priority 1 finding, or more than one Priority 2 findings and Priority 3 findings. - Priority 2 and 3 findings only where the cumulative financial impact is significant. - Corrective action and oversight by senior management is required. - Audit findings will be subject to a follow-up by Internal Audit.
Immediate Action Required	- Key controls are either not adequately or appropriately designed and are not operating effectively, or there is an absence of appropriate key controls to support objectives and manage risks. - More than one Priority 1 finding, combined with Priority 2 or 3 findings. - Regardless of the type of findings, the cumulative financial impact is material to the City's financial statements. - Confirmed fraud by management or staff. - Corrective action and oversight by Corporate Leadership Team is required immediately. - Follow-up of such audit findings by Internal Audit would be of high priority.

Appendix B: Criteria for Evaluating Audit Findings

Priority 1 (P1)

One or more of the following conditions exist that require **immediate attention of the Corporate Leadership Team**. Corrective actions by senior management must be implemented.

- Financial impact of both actual and potential losses is material.
- Management's actions, or lack thereof, have resulted in the compromise of a key process or control, which requires immediate significant efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks. Failure by management to remedy such deficiencies on a timely basis will result in the City being exposed to immediate risks and/or financial loss.
- One or more of the following conditions is true: i) management failed to identify key risks; ii) management failed to implement processes and controls to mitigate key risks.
- Management's actions, or lack thereof, have resulted in a key initiative to be significantly impacted or delayed, and the financial support for such initiative will likely be compromised.
- Management failed to implement effective control environment or provide adequate oversight, resulting in a negative pervasive impact on the City or potential fraudulent acts by City staff.
- Fraud by management or staff, as defined by the Corporate Fraud Prevention Policy (policy 2.14).

Priority 2 (P2)

One or more of the following conditions exist that require attention by senior management. Corrective actions by management should be implemented.

- Financial impact of both actual and potential losses is significant.
- Management's actions, or lack thereof, may result in a key process or control to be compromised, which requires considerable efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks.
- Management correctly identified key risks and have implemented processes and controls to mitigate such risks, however, one or more of the following is true: i) the processes and controls are not appropriate or adequate in design; ii) the processes and controls are not operating effectively on a consistent basis.
- Management's actions, or lack thereof, have impacted or delayed a key initiative, and the funding for such initiative may be compromised.
- Management failed to provide effective control environment or oversight on a consistent basis, resulting in a negative impact on the respective division, or other departments.
- Management failed to comply with Council-approved policies, by-laws, regulatory requirements, etc., which may result in penalties.
- Management failed to identify or remedy key control deficiencies that may impact the effectiveness of anti-fraud programs.

Priority 3 (P3)

One or more of the following conditions exist that require attention by management. Corrective actions by management should be implemented.

- Financial impact of both actual and potential losses is insignificant.
- A non-key process or control if compromised may require some efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks.
- Processes and controls to mitigate risks are in place; however, opportunities exist to further enhance the effectiveness or efficiency of such processes and controls. Management oversight exists to ensure key processes and controls are operating effectively.
- Minimal risk of non-compliance to Council-approved policies, by-laws, regulatory requirements, etc.
- Low impact to the City's strategic or key initiative.
- Low impact to the City's operations.

Appendix C: Three Tier Support Structure

The City of Brampton's internal IT customer service structure is built on a generally-accepted three-tier support model for IT Service Management. The following is a general description:

Tier 1: This is the basic level of customer support and it is where the Service Desk function is situated. This tier fields incoming customer communications such as telephone calls or email requests. This level tends to be reactive and real-time. Any issue that cannot be resolved at this level is escalated to Tier 2.

Most Service Desks provide some level of technical support, with the aim of resolving common issues at the first-line and reducing the amount of issues that are escalated to Tier 2 or Tier 3.

Tier 2: This level of support is often closely associated to the Service Desk, but with deeper general or specialized skills. There tends to be fewer issues residing at this level, and they typically take more time to resolve. Tier 2 support staff often have additional technical training and are able to resolve more complex issues.

Tier 3: At this level of support, specialist support teams focus on specific technologies and applications. Only properly triaged issues should be escalated to Tier 3. Issues may be assigned to Tier 3 directly from Tier 1 or may have been escalated from Tier 2.

KPMG

Appendix D: Table of KPMG Findings and Recommendations, and City Management Responses

#	Risk	Issue	Recommendation	Management response, executive and deadline
1	● (two)	**Out of hours system issues are not recorded**	We recommend that management re-enforce the policy with all staff who can raise tickets related to system outages, to ensure all system issues result in a HEAT ticket and follow the monitoring and escalation procedures. The monitoring systems should have alerts defined that result in the automatic generation of event or incident tickets on HEAT. The weekly reports of incidents and events should include a separate section on out of hours incidents raised.	**Management Response Including Timeline** Updates to the Incident Process are currently underway, this will reinforce the need for incident tickets to be created. Targeted completion end of March 2019 In addition, we are investigating the ability to have ticket creation integrated with the infrastructure monitoring tools. Targeted completion December 2019. Will review and introduce the ability to generate reports that separate out of hours incidents raised. Target completion March 2019.
		Tickets for “out of hours” system issues or events are not being recorded on the HEAT ticketing system. “Out of hours” support refers to support between 4:30 PM and 8:30 AM and the weekend. Alerting systems are in place in the datacentre to monitor for outages and events, and the IT team directly monitors systems using email and text alerts. However, any “out of hours” outages are not being recorded as tickets in HEAT at the time they occur, either by automated or manual methods. The monitoring systems do not appear to have any alerts defined that result in the automatic generation of event or incident tickets on HEAT. All outages should be identified and escalated through the proper channels to the right stakeholders. Currently, there is no policy in place, describing the required activities, outage conditions, escalations channels and relevant stakeholders. We are advised that management raise incidents the day after out of hour’s incidents, however, these cannot be identified on the HEAT system. There is a risk that oversight and accountability for the process of managing incidents for out of hour’s systems issues cannot be established while they are not being recorded on HEAT. Not properly recording and escalating system issues could lead to lack of oversight, insufficient prioritization, longer resolution times, and impact systems availability. In addition, the effort involved in supporting systems out of hours is not visible at present.		
2	● (two)	**Mandatory Service Desk ticket fields are not always populated**		

#	Risk	Issue	Recommendation	Management response, executive and deadline
		Out of 30,052 tickets reviewed from October 1, 2017 to September 30, 2018, 2,656 tickets did not have the field for category, priority or both populated, for both incident and request type tickets. The HEAT system is set up to provide dropdown menu options for these fields. However, it appears that the dropdown facility is not always operating correctly. Although we observed the expected error messages appearing when the dropdown was not completed correctly by the user, the root-cause for this issue has not been established. It is not possible to ensure service level agreements are complied with, when the category and priority fields are not populated correctly. This could result in high priority incidents not being identified and addressed correctly and in a timely manner, potentially adversely impacting system availability at City of Brampton.	We recommend that the root-cause for the dropdown facility not operating correctly is established and remediated.	**Management Response Including Timeline** Updates to Incident Processes are underway. We will enforce the process once documentation and training for staff is complete to include categorization. Targeted for end of March 2019 A new or updated tool for incident management is being investigated and targeted for production implementation by the end of year 2019. SLA integration is scheduled with the new or updated tool, listed above, for end of year 2019
3	● (two)	**Low priority ticket SLA's are being breached**	We recommend that the protocol for monitoring and addressing breaches is strengthened through additional training and improved escalation of reporting of breaches. Tickets that are at-risk of breaching the SLA should be monitored and addressed, to prevent breaches.	**Management Response Including Timeline** Queue Management practices are currently being redefined and enforced through proper queue management processes, metrics, implementation of KPI's and Management escalation, so tickets do not breach. Target completion – April 30th 2019 In addition, further training of the management of a given ticket will be done for queue managers (train the trainer style) and Client Care Staff. Target - spring 2019. New Management dashboards for Queue Managers and Senior managers as needed, are being designed to identify
		Out of 30,012 tickets reviewed from October 1, 2017 to September 30, 2018, 2,161 tickets were not resolved in line with the timeframe outlined in the terms of their Service Level Agreement (SLA). Breaches of SLA account for about 7.2% of the total closed and resolved tickets. We observed that only lower priority ticket (priority 3, 4, and 5) were breaching their SLA, with the lowest priority tickets have the highest number of breaches. Low priority tickets raised can be symptomatic of higher priority system issues. There is a risk that serious issues may not be identified in time, if large numbers of low priority issues are not resolved in a timely manner.		

#	Risk	Issue	Recommendation	Management response, executive and deadline
				tickets that are approaching SLA breaches. Targeted May 2019
4	● (two)	**Breaches and tickets-at-risk listed in weekly reporting are not addressed**	We recommend that the role of the monitor is enforced and the protocol for addressing breaches is strengthened through additional training and improved escalation of reporting of breaches. Tickets that are at-risk of breaching the SLA should be monitored and addressed, to prevent breaches. In addition, we recommend that reasons for breaches are standardized, for management to be able to report and address the reasons. Adding a specific field to the ticket form in HEAT could for instance capture this reason.	**Management Response Including Timeline** Following the updated incident process documentation we will be conducting additional training with the queue managers (those that have a queue to manage with staff and ticket flows) to better understand the process for ticket management – targeted for June 2019 In addition, weekly metrics and follow up will be implemented for the queue Managers in order to identify targets. Targeted August 2019
		Although there is weekly reporting to inform team managers of open tickets and service level agreement breaches, no follow up action is tracked to address breaches which results in tickets remaining open without being addressed in a timely manner. Management advised that there is a protocol in place where a person is assigned to act as a monitor and address tickets at risk of breaching the SLA or actual breaches. There is no evidence of the escalation process in the reports. Notes of activities performed on tickets are captured in the history field, which is a free format field. The reason for breaches should be captured and standardized, in order to report and address the reasons. Not addressing tickets at risk of breaching SLA or actual breaches, could lead to (further) adverse impact on the systems. Low priority breaches could turn into higher priority issues.		
5	● (two)	**There is no explicit policy for event, problem and request management in place**	We recommend that responsibilities for raising and managing events and problems are defined, to ensure the right person is notified to resolve the ticket. The definition of a system event is not clearly stated in the CoB Incident Management Process Guide and should be updated. ITIL defines system events as a change of state that has significance for the management of an IT service or other configuration item (CI).	**Management Response Including Timeline** Incident Management process guide is currently being updated and improved. Targeted completion end of March 2019. Service Request Management enhancement training will take place for those Queue Managers and staff that handle Service requests. Targeted for August 2019 In addition, the implementation and integration with Service Request Mgmt
		The COB Incident Management Process Guide refers the different types of tickets including events, incidents, problems and requests as follows: - Event: events that do not indicate exception to normal service operation and are not determined significant by the Event correlation engine. - Incident: any event which disrupts, or has the potential to disrupt an IT service and associated business processes. - Problem: (major) incidents that require a root-cause analysis.		

#	Risk	Issue	Recommendation	Management response, executive and deadline
		- Request: a service request that does not involve any (potential) disruption to an IT service. For this review, we define events as system events, as only IT control related events are typically tracked and managed by IT. Event Management is not done in City of Brampton, and events are not found in the HEAT ticketing system at present, as there is no facility in the tool to manage events. There is no guidance for raising and managing events or problems, including details of who should be responsible for the various types of events and problems that are raised. There is no specific guidance available for request management. Management advised that guidance on request management is encompassed within the guidance for incidents, but not all incident related guidance is applicable to requests and it is not always clear if guidance should be applicable for requests as well. There is a risk that unclear assignment of responsibilities for different types of tickets, or the use of the wrong ticket type could negatively impact the resolution of the different types of tickets. There is a risk of staff being unaware of the ticket, tickets being raised incorrectly or the wrong person being assigned to address the ticket. Missing guidelines on the differences in identifying and handling the different types of tickets, could lead to missing tickets or incorrect prioritization and resolution.	Furthermore, the distinction between requests and incidents should be clear, for instance by establishing a separate request management policy. In addition, we recommend that guidelines are established on the differences in identifying and handling the different types of tickets, to ensure tracking is performed and the tickets are prioritized and resolved correctly.	software, of a broader intake process for all requests received by the division, will help identify and categorize Service requests as project or operational. Projects will be further defined as capital budget request or current project change request. Integration with intake tools needs to be done. Using Intake to determine service requests that are net new development. A manual process is in place currently that will be documented as a process by mid March 2019. Integration is targeted December 2019
6	● (two)	**Process awareness and training can be improved**	We recommend scheduling periodical updates or trainings for Service Desk staff, to discuss updates to the operational procedures and the results from problem management.	**Management Response Including Timeline** Periodical updates will start and be continuous as the Knowledge Articles mature. Staff training is ongoing at monthly team meetings with Client Care staff, periodic updates are sent via email to staff
		Staff working on the Service Desk are not being trained regularly about changed processes, resolutions to incidents or new project developments. Staff should be made aware of results and learnings from root-cause and trend analyses from problem management, significant projects or any organizational developments. There is a HEAT document, describing how to use HEAT, but the document is only shared upon request with IT Service Desk staff. There is also an extensive knowledge		

#	Risk	Issue	Recommendation	Management response, executive and deadline
		base, which describes the solutions for different incidents. The knowledge base documents are maintained by the Service Desk Coordinator. Updates to the knowledge base are communicated to the Service Desk staff through weekly emails and alerts, but there is no update training performed for major changes or developments. Without training staff on updates, new operational procedures may be inconsistently performed or not performed at all. Experienced staff tend not to consult the knowledge base for common incidents or requests, which means they may be unaware of updates resulting in out of date procedures being used to address incidents.		regularity and stored on the client care site. More formal rigor will be implemented in the following manner: - Knowledge Articles are updated and completed for all existing service offerings – target end of June 2019 - Transition to Operations process is in place for net new services to include the creation of a Knowledge article and the subsequent training of Client Care staff to support – targeted end of June 2019 - A new or updated tool for ITSM as a whole, which includes a detailed CMDB which is automated to search for a known error or Knowledge Article to assist Client Care staff as they create an incident, improving first point of contact resolution – targeted for end of December 2019
7	● (two)	**Not all incidents/requests are being reported**	We recommend that the policy of documenting and tracking all events is being reinforced with all Service Center and Service Desk staff and is being monitored for adherence.	**Management Response Including Timeline** Senior management supports the need for incidents to be raised by all when there is an interruption or degradation of service. A new ITSM process manager is in place as of December 2018 to explore these gaps and ensure we close them. A log as been created at the Service Center to track walk in clients and ensure tickets are entered for everything. Completed January 2019. With the new or upgraded tool, we will look into creating an automated system
		During the course of our review, we noted two separate events that did not result in a ticket in the HEAT system. Both these cases were raised at the onsite Service Center. Not documenting and registering all events, could lead to incorrect resolution or SLA breaches and no insight in the actual workload of the Service Desk and nature of the events.		

#	Risk	Issue	Recommendation	Management response, executive and deadline
				for the service center, so that nothing gets missed and tickets are generated for all. Targeted end of December 2019. Consideration to move service center to appointment only with a valid incident ticket or service request is underway. Analysis should be completed by end of March 2019
8	● (two)	**Problem management is not fully being performed**	We recommend that the responsibilities for handling problems are established, to ensure the root-cause of problems is reviewed and trends over time are analyzed. Possible improvements for resolution or employee training should instigated when possibilities are found to prevent or mitigate incidents.	**Management Response Including Timeline** A new ITSM process manager is in place as of December 2018 to explore these gaps and ensure we implement ITSM/ITIL standards as they are intended, including and not limited to complete problem management. Process review, update and finalization will be completed by end of April 2019.
		Problem management practices at the City of Brampton is not mature. At present there are a total of 20 problems on the HEAT system. These are related to incidents which have been grouped into a single problem by a Service Desk Coordinator. There is no separate IT application team who are assigned problems along with incidents related to their application or area of expertise. Identification and remediation of the root-cause activities does not appear to be taking place. The problems are marked as active and most are older than 6 months, indicating that new problems are not being regularly identified. In addition, we noted that there is no analysis performed on trends over time and as such there is no learning from incidents. Not addressing or identifying the root-cause of problems and analyzing trends over time, could mean opportunities to prevent incidents or mitigate the impact are missed.		
9	● (three)	**The ticketing facility is not always used as designed, as certain tickets are raised 6 months in advance.**	We recommend that these 'placeholder' requests are either not tracked in HEAT or HEAT is to be updated to start measuring SLA once relevant opposed to at incident start. It should be investigated if such placeholders should be set up as events instead.	**Management Response Including Timeline** Placeholders should never be entered and tracked in HEAT. This is under investigation and will be managed on a project by project basis until the
		Of the 1,644 breached service request tickets, we were informed that among these tickets there are 'placeholder' tickets for requests or activities that are due in the future and cannot be executed until a future date. Often these can be up to 6 months in the future. The current ticketing facility does not differentiate between these 'placeholder'		

#	Risk	Issue	Recommendation	Management response, executive and deadline
		tickets and regular tickets, meaning all tickets are treated as the same and follow the same tracking mechanisms. This means overviews and reports are incorrect. Having these 'placeholder' tickets on the system, affects oversight and tracking activities, as the data is incorrect. Incorrect overviews and reports, could lead to tickets breaches or incorrect prioritization.		implementation of a release management program scheduled for the fall of 2019.
10	● (three)	**Categorization can be improved** Tickets are grouped and categorized based on the following data fields: • Category: type of incident. • Configuration item (CI): specific reference to a system, workstation or other asset. • Service: what part of the main activities of user is affected. More than 50% of the incidents are categorized as 'Functionality'. Compared to categories as 'Connectivity' or 'Error Message', 'Functionality' seems a generic category. In addition, incidents affecting email can be referring to CI's 'Email', 'MS Outlook', 'Email - Mailbox' or 'Microsoft Outlook 2016', which when combined results in about 20% of all tickets. Effectiveness and efficiency of the Helpdesk process are negatively impacted by the current categorization practices. Timelines for resolving the incident are increased (as there are more possible solutions or knowledge base items that need to be considered) possible problems are not easily identified. In addition, ineffective categorization prevents in identifying possible self-service categories to improve overall efficiency and effectiveness of the IT helpdesk process.	The items currently listed in the field Category and Service should be evaluated and updated supporting clear categorization to help in resolving the incident quicker and identifying trends. ITIL guidelines can be used to evaluate the categories and adjust them to the practical situation of the City of Brampton. In addition, the list of CI's should be maintained and reviewed periodically on accuracy and possible overlap.	**Management Response Including Timeline** Management will take this into consideration when looking at the advancement of the tool being used for incident and problem management targeted for end of December 2019

BRAMPTON
Flower City
brampton.ca

Office of Internal Audit

Enhancement Required

November 30, 2018

Corporate Services Department

Digital Innovation and IT Division

Mobile Phone Management Follow-Up Audit Report

Executive Summary:

The 2018 Internal Audit Work Plan included a follow up audit of the 2017 mobile phone management audit.

The 2017 mobile phone management audit report had a rating of “Immediate Action Required”. The objective of the follow up audit was to ensure that management action plans related to findings from the 2017 audit report were effectively implemented. The follow-up audit period was from July 1st, 2018 to September 30th, 2018.

Mobile device technology is widely used in the City of Brampton and is integrated into key business processes. Reliance on the technology will continue to increase as the City’s data and technology environment continues to develop.

While this audit engagement focused on mobile telephone management, our current mobile telecommunication device inventory is comprised of 26% wireless network devices and tablets, and 74% mobile telephones. The wireless devices are used in laptops and specialized devices such as those used to record parking infractions.

Appendix C details the 2017 and the 2018 audit findings.

Overall Results:

The overall risk profile associated with mobile telephone management has improved. Operational management and cost recovery actions have been completed, but enhancements are still required around oversight, strategy, asset management and user off-boarding. The quarterly reimbursement process for personal use was implemented in July 2018: however, effectiveness testing could not be performed as the repayment cycle would occur after the audit period. Additional roaming options should be investigated as should opportunities for process and report automation.

Background:

The Digital Innovation and Information Technology Division (“IT”) of the Corporate Services Department is responsible for the management of mobile telecommunication services of the City of Brampton (“City”), as well as the provisioning of mobile phones.

The City leveraged Province of Ontario Agreement available to the Broader Public Sector (including municipalities), through the Ministry of Government Services for telecommunication services. The agreement allows the City to take advantage of the large volume discounts generated by the Province. Effective May 1, 2014, the City contracted Rogers Communications (“Rogers”) as its primary wireless mobile cellular service provider. A small number of network devices remain with Bell Mobility (“Bell”).

The renegotiated Provincial plan came into effect on July 1, 2018. As a result, the average usage cost per mobile phone device for the month of September 2018 was $20.24, the lowest cost based on a 12 month review of average monthly costs, with the highest cost at $29.24 in May 2018 under the old plan. Some of the highlights of the current July 1st 2018 plan that contributed to the reduction in average cost:

- The current data plan costing $14.30 includes 6 GB of data. The previous data plan was a stacked plan that started at $15.25 for the first 300Mb, increased to $30.00 after 300 MB, and then increased to $45.00 after 1 GB;
- Canadian long distance charges are now $0.01 per minute, with the option to add unlimited minutes for $3.13. These costs were $0.02 and $6.00 respectively in the previous plan;
- Unlimited Multimedia Messaging Service (MMS) and texting is now included.

See **Appendix D** for details of the current price plan.

The Finance Division and IT updated processes on July 1st, 2018 that provide more oversight of personal usage. The net result was increased reimbursement to the City for personal usage.

Mobile Device Inventory

As of the end of September, 2018, the City possessed a total of 1,473 mobile devices, including networking devices, telephones and tablets.

Table 1 is an analysis of the current inventory, showing the total count and usage cost of all devices, categorized by service and carrier. Networking devices, which includes tablets, make up 26% of the inventory. This represents a 112% increase in one year, as presented in **Table 2**.

Table 1: Total count and costs by service and carrier for September 2018

Service	Carrier	Number of Devices	% of Total Number of Devices	Total Expenses	% of Total Expense
Network Devices	Bell Mobility	54	3%	$ 1,429	3%
Network Devices	Rogers Wireless	307	21%	$ 5,166	11%
Smartphones	Rogers Wireless	922	63%	$ 38,169	83%
Network Devices-Tablets	Rogers Wireless	27	2%	$ 419	1%
Voice	Rogers Wireless	163	11%	$ 1,036	2%
Totals		1,473	100%	$ 46,219	100%

Table 2 shows the inventory changes over September 2017 and September 2018. The total number of devices increased by 17%. The corresponding cost increase was 8% as the total expenses for September 2018 was $46,219 while that of September 2017 was $42,864.

Table 2: September 2018 inventory vs 2017

Service	Total Number of Devices September 2017	Total Number of Devices September 2018	+/- % Change
Network Devices	147	361	146%
Smartphones	895	922	3%
Network Devices-Tablets	42	27	-34%
Voice	179	163	-8%
Totals	1,263	1,473	17%

Mobile Telephone Usage

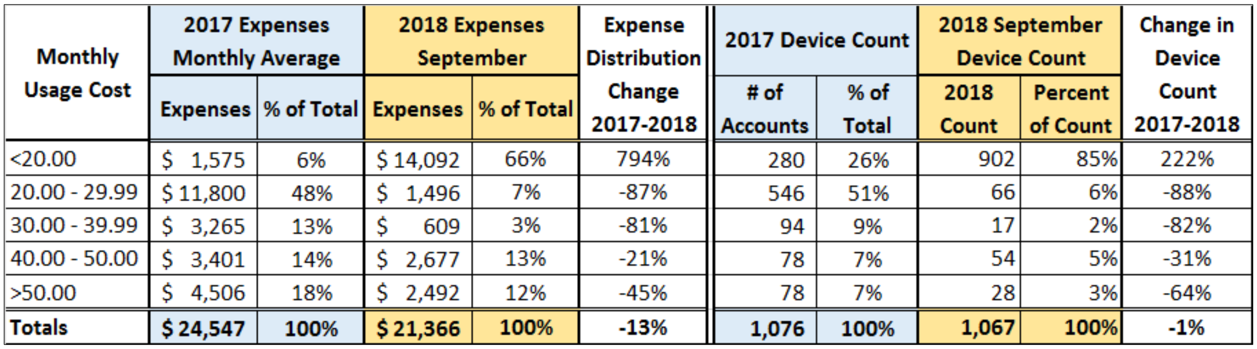
As of September 2018, the City had a total of 1,067 mobile phone accounts, which includes smart phones and voice phones; and, excludes networking devices, cancelled plans, and plans for Members of Council. Costs are limited to phone usage and excludes charges such has the cost of new telephones.

Table 3 provides an analysis of September 2018 mobile phone usage in comparison to the 2017 mobile phone statistics.

The following items should be noted:

- The number of monthly plans that remained under $20 has increased from 280 to 902 devices over the year.
- While the total number of mobile phones decreased by 1% in September 2018, the cost decreased by 13%.
- The 2017 audit reported that 7% of users exceeded $50 a month in usage costs. This decreased to 3% in September 2018.

Table 3: Average Monthly Mobile Usage 2017 Audit Compared to Sept 2018[1]



Monthly Usage Cost	2017 Expenses Monthly Average		2018 Expenses September		Expense Distribution Change 2017-2018	2017 Device Count		2018 September Device Count		Change in Device Count 2017-2018
	Expenses	% of Total	Expenses	% of Total		# of Accounts	% of Total	2018 Count	Percent of Count	
<20.00	$ 1,575	6%	$ 14,092	66%	794%	280	26%	902	85%	222%
20.00 - 29.99	$ 11,800	48%	$ 1,496	7%	-87%	546	51%	66	6%	-88%
30.00 - 39.99	$ 3,265	13%	$ 609	3%	-81%	94	9%	17	2%	-82%
40.00 - 50.00	$ 3,401	14%	$ 2,677	13%	-21%	78	7%	54	5%	-31%
>50.00	$ 4,506	18%	$ 2,492	12%	-45%	78	7%	28	3%	-64%
Totals	**$ 24,547**	**100%**	**$ 21,366**	**100%**	**-13%**	**1,076**	**100%**	**1,067**	**100%**	**-1%**

---

[1] The September results are representative of the 2018 third quarter results.

Total Departmental Spending

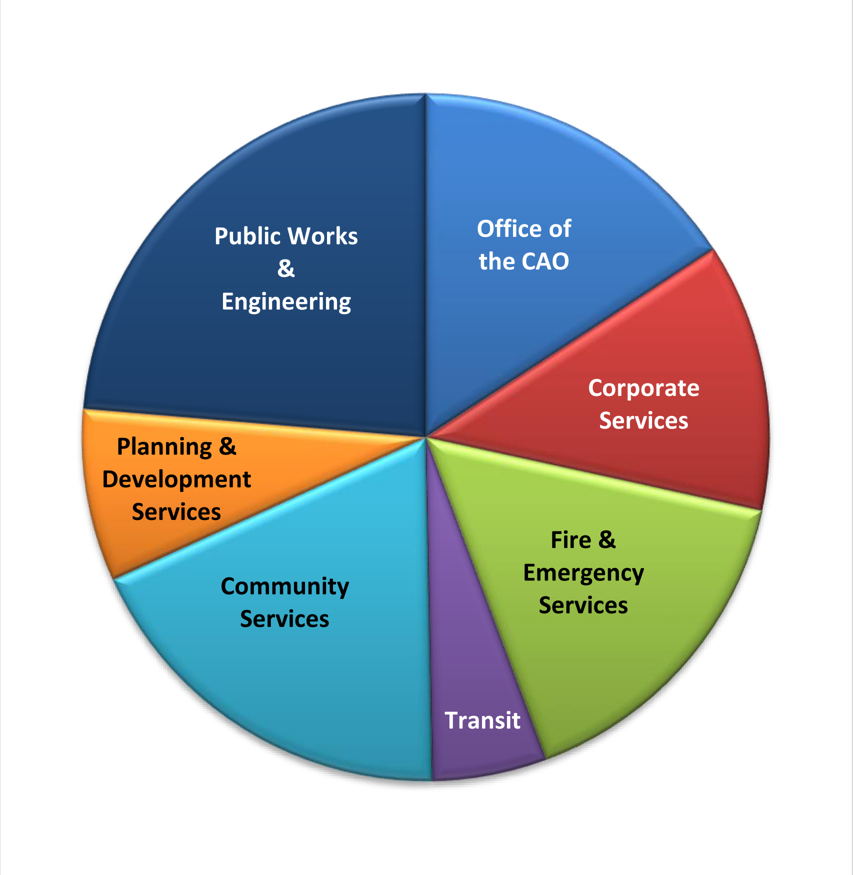
In the following exhibits, **Chart 1**, **Table 4** and **Table 5** show total departmental spending on mobile phones.

Of the total cost of $35,385 for September 2018[1], approximately $14,929 related to equipment and features charges. Equipment costs vary month to month based on when a phone is purchased, and these averaged $14,000 per month over the last year.

Given that the third quarter of 2018 was a transition period, there is insufficient data to establish the longer term impact of the changes resulting from the new mobile phone plan.

Chart 1 below is a visual representation of the data in **Table 4**.

Chart 1: Mobile Telephone Expenses by Department – September 2018



---

[1] This represents all mobile phone accounts, less one time accounts created for the Election.

Table 4: Mobile Phone Expense by Department - September 2018

Department	Total Mobile Phone Expense
Office of the CAO	$ 5,583
Corporate Services	$ 4,476
Fire & Emergency Services	$ 5,626
Transit	$ 1,897
Community Services	$ 6,553
Planning & Development Services	$ 2,875
Public Works & Engineering	$ 8,375
Total	$ 35,385

Table 5 compares the departmental cost ratio presented in the 2017 mobile phone audit to the third quarter 2018 mobile costs.

Table 5: 2017 and 2018 Mobile Expense Ratios Compared

Department	2017 Complete Mobile Phone Expenses[1]	2018 / Q3 Mobile Phone Expenses[2]	% Change
Office of the CAO[3]	10%	13%	3%
Corporate Services	21%	16%	-6%
Fire & Emergency Services	8%	8%	1%
Transit	7%	5%	-2%
Community Services	27%	24%	-3%
Planning & Development Services	5%	7%	2%
Public Works & Engineering	23%	27%	4%

Notes: [1] The 2017 percentages are based on twelve months of data.

[2] The 2018 percentages are based on Q3 2018 data.

[3] In order to better compare the 2017 and 2018 numbers, we included Economic Development and Culture expenses in the Office of the CAO.

Audit Scope and Objectives

The objective of this engagement was to assess the implementation of management action plans to address the findings from the 2017 audit. Specifically, we assessed whether:

- Corporate mobile phone approval, acquisition and deactivation processes are adequately managed and controls are effective; and,
- Personal usage and charges are adequately monitored and reimbursed within established, appropriate policies and standard operating procedures.

Our audit scope included the following:

- Mobile phone approval, acquisition and deactivation processes;
- Personal phone data and charges;
- Review of the agreements with mobile device and service providers;
- Review of the agreements with wireless telecommunication expense management solution provider; and,
- Data security controls.

Not included in the scope of this audit were:

- Corporate landlines;
- Bring Your Own Device cell telephones;
- Compliance with Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
- Disposal of mobile telephones;
- Monthly mobile phone charges and invoice payment processing controls;
- Initial hardware costs of mobile phones; and,
- Mobile usage data of the Mayor and Counselors.

Findings:

1. Insufficient management oversight

Priority 2

Management has undertaken a preliminary assessment of data processing security and integrity. Management works with any third party vendors to address operational issues and relevant oversight reports are reviewed by management. However, management has not completed annual vendor evaluations or a security assessment. In order to ensure City standards are maintained, both items should be completed by management.

Recommendations:

1. Management should perform a third party security assessment.
2. If a third party is to be engaged, management should assess and evaluate their control environment to ensure data governance security and stability. In addition, regular third party vendor reviews should be undertaken and a right to audit clause should be included in all contracts.

Management's Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	Security assessment framework is being developed for vendors.	Manager – Security & Risk	Q3 2019
2	Recommendations from the security assessment will be followed.	Manager – Immersive Technologies	Q3 2019

2. Insufficient asset management controls

Priority 2

Work is required to establish mobile asset management controls. There were 95 active mobile phone assets linked to Rogers's telephone numbers not listed in an internal mobile device inventory. An additional 201 mobile networking devices could not be located in the inventory lists. The internal City inventory included: spreadsheets that track voice-only mobile phones; the Blackberry Enterprise Server (BES); and, the inTune mobile phone management tools.

Recommendations:

1. Management should assess asset management tools to consolidate and manage all mobile device assets.

Management's Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	The IT strategy will review the mobile asset management policy for further enhancement, to enable a better approach to mobile asset tracking and management. Currently all Mobile Phones and the numbers (SiM) are tracked by tools like inTune. Rogers tracks the mobile number. The Blackberry devices are tracked in BES system and are being phased out in 2019. Once this is done then the BES system will no longer be required. We are also following the mobile number cancellation process which are notifications sent out to the departments every 30/60/90 days. Once a comprehensive mobile asset management strategy is in place, IT will align.	CIO	Q1 2020

Priority 2

3: Inconsistencies and gaps in the employee off-boarding process

Effective employee off-boarding has not been established:

- IT is not consistently being notified of staff departures, job reassignment, leave of absence, and leaves resulting in departures;
- Regular management review of active employees and the tools and technology required for their roles is not in place;

- Not all inactive devices identified in the Zero Usage Reports are released by management to be redeployed; and,
- Mobile devices are not consistently retrieved along with computers and other assets when an employee is not longer active or employed by the City.

Twenty-two (22) mobile phones were found registered to former employees. These former employees left the corporation between January 28, 2017 and July 11, 2018 incurring a cost of $2,432.

Recommendations:

1. Management should work with Human Resources (HR) to review and update the off-boarding process to ensure IT is consistently notified of any employee status change so that:
    - The necessary system accounts are updated;
    - The asset inventory is updated; and,
    - Mobile technology assets are retrieved.

   A status change includes staff departures, job reassignment, leave of absence, and any leaves resulting in departures.
2. Ensure inactive devices identified by the Zero Usage Report are released and re-assigned to active employees.
3. Consider annual management acknowledgement of active assets and periodic management review of staff system access permissions.

Management's Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	Off-Boarding is a corporate wide initiative and DI&IT is one of the impacted divisions. When this process is updated, DI&IT will align to the off-boarding process. We will actively champion and represent these types of issues as part of process rework.	CIO	Align with HR review timelines
2	As part of the overall IT Asset management process, IT will ensure that inactive devices are either released or reassigned to active employees.	Manager – Immersive technologies	Align with IT strategy timelines
3	IT Security team is developing a security and risk management plan, which covers system level access permissions.	Manager – Security & Risk	Q1 2020

4: The current mobile device technology management processes do not reflect the changing environment

Priority 2

There is no policy in place to establish, guidelines and expected practices relating to mobile device technology management. The findings in this report related to asset management, user device management and mobile data management are reflective of a lack of defined principles. In addition, the management of mobile assets is not consistent with the management of other corporate IT assets, such as laptops and computers.

The mobile device technology landscape within the City is changing. Wireless networking devices account for 26% of the City's mobile devices, a 112% increase from the 2017 audit. Without a policy in place expected practices are not defined and cannot be consistently applied.

Recommendation:

1. A mobile device technology policy should be developed to ensure consistency, provide guidance and establish accountability.
2. A mobile device technology strategy should be established to support the City's changing use of mobile technology.

Management's Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	The "Administrative Directive" for the use of Information technology resources has been drafted and will go to SLT for approval March/April 2019. This addresses mobile device usage and provides high level guidelines We do see the lack of a corporate mobile device policy. However, currently, there is an IT use policy available – Policy No. 2.11.0. which is applied to users within City of Brampton. We will work to develop a comprehensive mobile device policy by Q4 2019	CIO	Q4 2019
2	DI&IT will align with the corporate mobile strategy.	Manager – Immersive Technologies	Q4 2019

5. Potential for increasing roaming costs and insufficient pricing options

Priority 2

The current “stacking” roaming plan (Appendix D) is the only option available and provides ease of use. However, controls to assist users in managing data usage do not exist.

No alerts are provided to users that they are reaching usage cost thresholds. There is no limit as to how much a user may be charged on this stackable plan.

An assessment of roaming costs could not be performed as the current plan was effective from July 2018 and third quarter costing and reimbursement information was not available at that time.

Recommendation:

1. Management should investigate the availability of different roaming options or add-on plans to give employees choices to managing their roaming costs.
2. Management should investigate options such as alerts to notify users they are reaching price increase thresholds.

Management’s Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	At the inception of the contract the only roaming options was the stackable option. After Rogers received feedback from the Province and Brampton, other options were made available in 2019. These other options are not yet communicated as they are under review. These other options will require lead time from users to allow DI&IT to connect with Rogers.	Manager – Immersive Technologies	Q2 2019
2	Rogers introduced alert notifications to users in February 2019. These are being implemented and a communications plan is being drafted for released to all users via the Departmental Designates. The alerts are sent via text messages to users.	Manager – Immersive Technologies	Q2 2019

6. Personal usage reporting is a manual process and is unsustainable

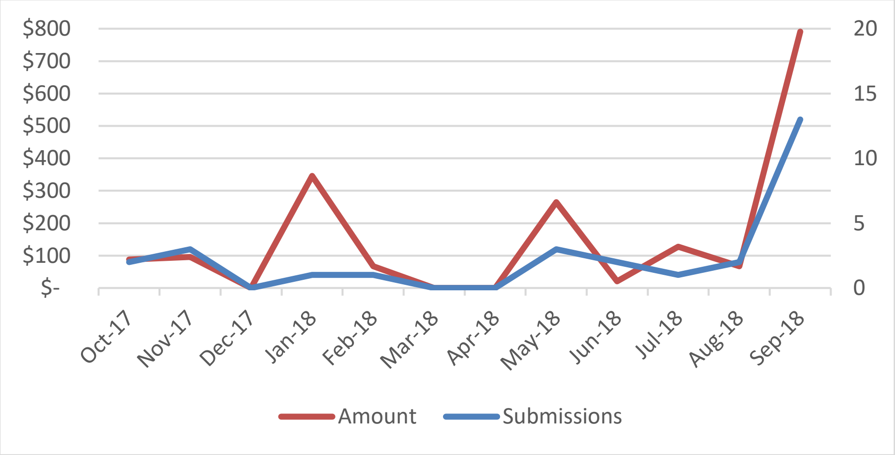
Priority 2

The process implemented in July 2018 to recover personal usage costs is manual and the creation of the usage reports is labour intensive. While this process provides management with the necessary oversight it cannot be sustainable over the long term.

While roaming and long distance costs that were confirmed personal in nature were identified during the audit, reimbursement could not be validated as the reimbursements would be made subsequent to the audit period.

The Finance Division and the Digital Innovations and IT Division jointly updated processes in July 2018 to improve cost recovery for excessive personal use of mobile phones. See **Chart 2**. As a result of the new processes, 13 reimbursements totaling nearly $800 were made in the month of September 2018 alone.

Chart 2: Changes in personal reimbursements, by month



Recommendation:

1. Management should consider automating both the quarterly reporting and reimbursement processes.
2. Management should consider creating key performance indicators related to reimbursement of personal usage costs in order to assess adherence to the SOP.
3. Management should consider using predictive analytics to develop exception reporting.

Management's Response:

Rec. #	Action Plan	Person Responsible	Target Date
1	As the contract with our current vendor comes up for renewal, we will revisit the potential of automating this process. The current process is a combination of Automated and Manual steps. The master report is automated. From the master report, sub lists are extracted for each department. These sub lists are sent via email and is a manual process.	Manager – Immersive Technologies	Q1 2020
2	Management agrees with the recommendation. Management will explore the feasibility of implementing key performance indicators related to reimbursement of personal usage costs in order to assess adherence to the SOP.	Senior Manager, Accounting Services & Deputy Treasurer	Q4 2019
3	IT will consider analytics based reporting to review exception reporting in the future	Manager – Immersive Technologies	Q1 2020

Conclusion:

The objective of this engagement was to assess the implementation of management action plans to address the findings from the 2017 audit.

There has been improvement noted as a result of the following changes and work performed:

- Mobile phones operating processes and procedures have been reviewed and updated and the device provisioning procedure has been automated;
- Mobile phone quarterly usage reporting has been implemented; and,
- The Personal Telephone Expenses SOP has been updated and communicated.

Insufficient action has been taken and as a result enhancements are still required in the following areas:

- Management oversight and strategy;
- Asset management; and,
- Employee off-boarding.

Effectiveness testing of personal reimbursements was limited as the updated controls became effective in July 2018.

As the City of Brampton increase its reliance on technology, the mobility device landscape will change. A corporate strategy and policy should be developed that embraces the changes anticipated and encompasses all mobile device technologies.

Appendices:

Appendix A: Criteria for Audit Report Rating

Appendix B: Criteria for Evaluating Audit Findings

Appendix C: Analysis of the 2017 and the 2018 Audit Findings

Appendix D: ROGERS Cellular Pricing Plans

Appendix A: Criteria for Audit Report Rating

The audit report rating is intended to provide management with an indication of the overall status of internal controls and processes in the audited area. The audit report rating is based on Internal Audit's overall assessment of the significance of issues identified during the audit process, and in conjunction with professional judgement also considers the following:

1. Design and effectiveness of internal controls, processes, procedures, policies, and systems.
2. Compliance with policies, standard operating procedures, and other requirements (i.e. legal, regulatory, accounting, contractual).
3. Quality of the data and information provided by management and related systems.
4. Efficiency of systems, processes and procedures.

Effective	- Key controls are adequately and appropriately designed, and are operating effectively to support objectives and manage risks. - Audit recommendations resulted in only minor enhancements to the effectiveness or efficiency of controls and processes. - One or more Priority 3 findings. - Insignificant cumulative financial impact when all audit findings have been considered. - Audit findings would not be subject to a follow-up by Internal Audit.
Enhancement Required	- A few key control weaknesses were noted that require enhancements to better support objectives and manage risks. - One Priority 2 finding and Priority 3 findings. - Priority 3 findings only where the cumulative financial impact is significant. - Corrective action and oversight by management is needed. - Audit findings could be subject to a follow-up by Internal Audit.
Significant Improvement Required	- Numerous key control weaknesses were noted that require significant improvement to support objectives and manage risks. - One Priority 1 finding, or more than one Priority 2 findings and Priority 3 findings. - Priority 2 and 3 findings only where the cumulative financial impact is significant. - Corrective action and oversight by senior management is required. - Audit findings will be subject to a follow-up by Internal Audit.
Immediate Action Required	- Key controls are either not adequately or appropriately designed and are not operating effectively, or there is an absence of appropriate key controls to support objectives and manage risks. - More than one Priority 1 finding, combined with Priority 2 or 3 findings. - Regardless of the type of findings, the cumulative financial impact is material to the City's financial statements. - Confirmed fraud by management or staff. - Corrective action and oversight by Corporate Leadership Team is required immediately. - Follow-up of such audit findings by Internal Audit would be of high priority.

Appendix B: Criteria for Evaluating Audit Findings

Priority 1 (P1)

One or more of the following conditions exist that require **immediate attention of the Corporate Leadership Team**. Corrective actions by senior management must be implemented.

- Financial impact of both actual and potential losses is material.
- Management's actions, or lack thereof, have resulted in the compromise of a key process or control, which requires immediate significant efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks. Failure by management to remedy such deficiencies on a timely basis will result in the City being exposed to immediate risks and/or financial loss.
- One or more of the following conditions is true: i) management failed to identify key risks; ii) management failed to implement processes and controls to mitigate key risks.
- Management's actions, or lack thereof, have resulted in a key initiative to be significantly impacted or delayed, and the financial support for such initiative will likely be compromised.
- Management failed to implement effective control environment or provide adequate oversight, resulting in a negative pervasive impact on the City or potential fraudulent acts by City staff.
- Fraud by management or staff, as defined by the Corporate Fraud Prevention Policy (policy 2.14).

Priority 2 (P2)

One or more of the following conditions exist that require attention by senior management. Corrective actions by management should be implemented.

- Financial impact of both actual and potential losses is significant.
- Management's actions, or lack thereof, may result in a key process or control to be compromised, which requires considerable efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks.
- Management correctly identified key risks and have implemented processes and controls to mitigate such risks, however, one or more of the following is true: i) the processes and controls are not appropriate or adequate in design; ii) the processes and controls are not operating effectively on a consistent basis.
- Management's actions, or lack thereof, have impacted or delayed a key initiative, and the funding for such initiative may be compromised.
- Management failed to provide effective control environment or oversight on a consistent basis, resulting in a negative impact on the respective division, or other departments.
- Management failed to comply with Council-approved policies, by-laws, regulatory requirements, etc., which may result in penalties.
- Management failed to identify or remedy key control deficiencies that may impact the effectiveness of anti-fraud programs.

Priority 3 (P3)

One or more of the following conditions exist that require attention by management. Corrective actions by management should be implemented.

- Financial impact of both actual and potential losses is insignificant.
- A non-key process or control if compromised may require some efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks.
- Processes and controls to mitigate risks are in place; however, opportunities exist to further enhance the effectiveness or efficiency of such processes and controls. Management oversight exists to ensure key processes and controls are operating effectively.
- Minimal risk of non-compliance to Council-approved policies, by-laws, regulatory requirements, etc.
- Low impact to the City's strategic or key initiative.
- Low impact to the City's operations.

Appendix C: Analysis of the 2017 and the 2018 Audit Findings

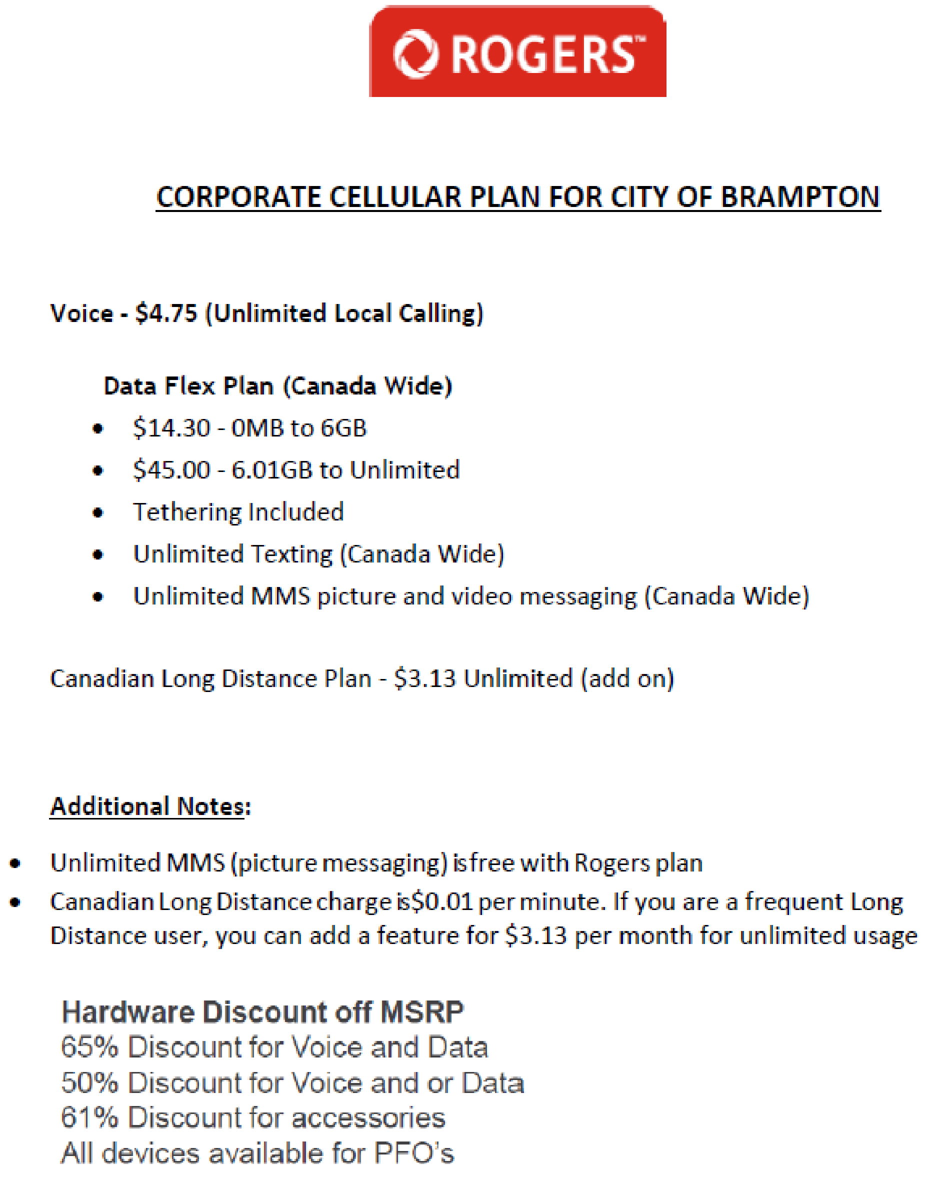
The table below compares the 2017 findings to the audit work performed in 2018 and shows the changes in priority rankings. See **Appendix A**: Criteria for Evaluating Audit Findings for an explanation of the P1 and P2 rankings.

2017 Ref #	Audit Rating 2017	Audit Findings 2017	Audit Rating 2018	Audit Findings 2018
1.	**P1**	There is a lack of management oversight of the mobile process to ensure City-provided mobile devices are not misused or misappropriated.	**P2**	Management oversight and operational processes have improved but some issues identified in the 2017 audit have not been addressed.
1.a)		Mobile phone process ownership is not assigned to a specific division. This has resulted in a lack of controls over the monitoring of mobile usage and misuse by employees.	**P2**	There remains a strategy and policy gap and the question of mobile phone process ownership has not changed. However, controls monitoring mobile usage and misuse by employees have been implement.
1.b)		There is a lack of information provided by IT management to increase the awareness of the mobile phone rate plans and provide guidance over acquisition, monitoring and deactivation of mobile telephones. This resulted in confusion and inconsistencies over the mobile phone process.	**Closed**	New and updated mobile phone maintenance procedures have been implemented and the provisioning procedure has been automated. The City is taking advantage of the Provincial agreement negotiated with Rogers Communication.
1.c)		There is no effective monitoring of excessive mobile usage by the operating departments. Based on the sample tested, personal long distance charges, roaming and other charges were identified that were not reimbursed to the City through Finance's reimbursement procedure as documented in the Personal Telephone Expenses standard operating procedures ("SOP").	**Closed**	Mobile phone usage reporting has been implemented, with management responsible for ensuring personal usage is reimbursed as per the Finance Personal Telephone Expenses SOP. Finance has communicated the updated Personal Telephone Expenses SOP and there has been an increase in reimbursements.
		Additionally, the City continued to pay for mobile charges after employees were no longer employed or were on leave of absence.	**P2**	Employee off-boarding is inconsistent. Periodic management reviews are not performed.
1.d)		There is no centralized database that manages and tracks mobile devices belonging to the City. As a result, corporate mobile asset management is ineffective.	**P2**	No change.
2.	**P1**	There is ineffective oversight by management over the agreement with or services provided by the solution provider. Management has not assessed the data security or integrity of the solution provider systems in handling sensitive mobile data of City employees.	**P2**	Management has undertaken a preliminary assessment of data security and integrity. However, management oversight is required to complete vendor evaluations and a security assessment.

Appendix D: ROGERS Cellular Pricing Plans

The following are images of the ROGERS pricing plans. Figure 1 shows the data, text and call pricing placed in Canada. Figures 2 provides a description of the roaming stacking plan and Figure 3 shows roaming costs for the United States and Europe.

Figure 1: Canadian Price Plan



ROGERS™

CORPORATE CELLULAR PLAN FOR CITY OF BRAMPTON

Voice - $4.75 (Unlimited Local Calling)

Data Flex Plan (Canada Wide)

- $14.30 - 0MB to 6GB
- $45.00 - 6.01GB to Unlimited
- Tethering Included
- Unlimited Texting (Canada Wide)
- Unlimited MMS picture and video messaging (Canada Wide)

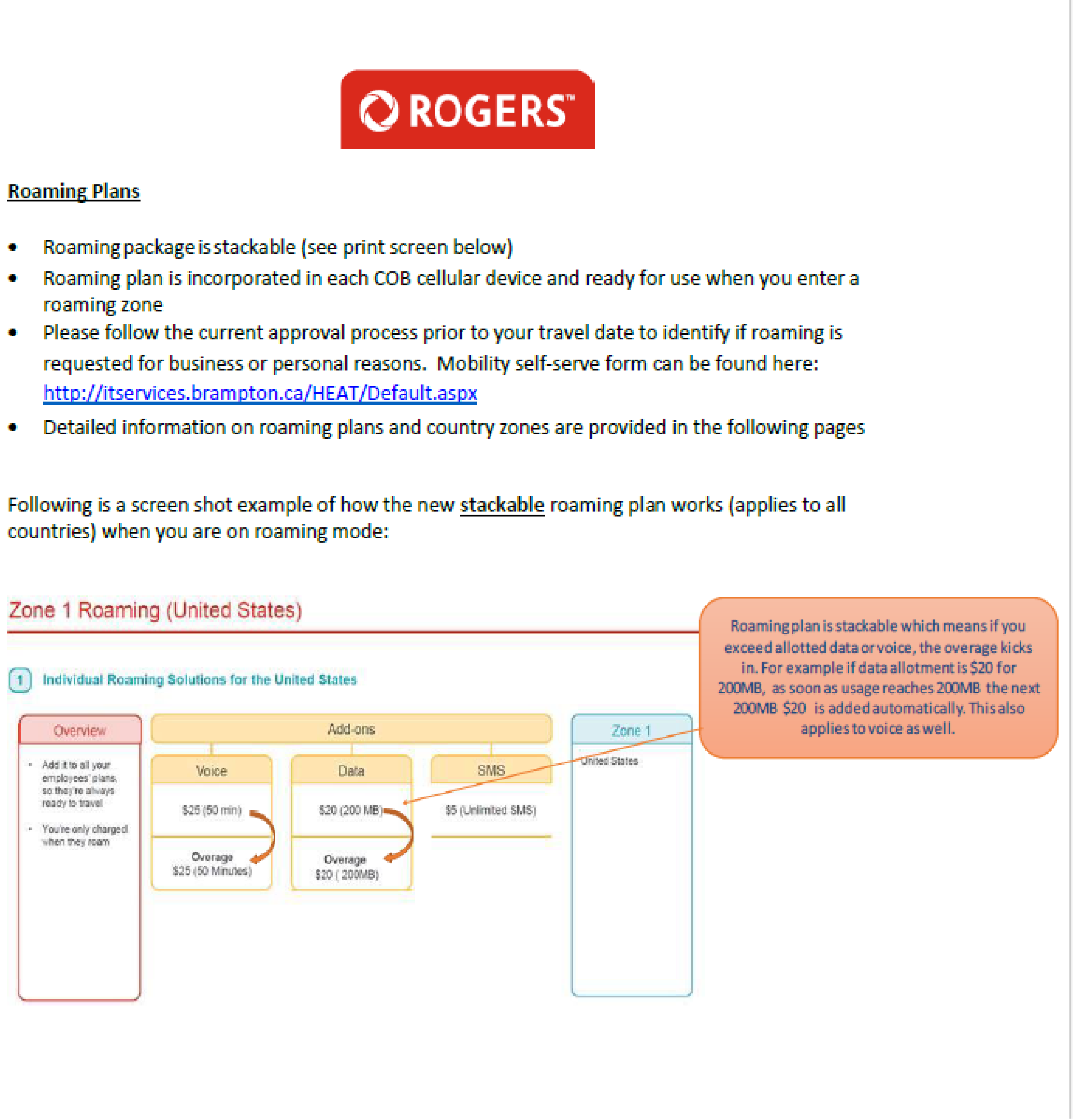
Canadian Long Distance Plan - $3.13 Unlimited (add on)

Additional Notes:

- Unlimited MMS (picture messaging) is free with Rogers plan
- Canadian Long Distance charge is $0.01 per minute. If you are a frequent Long Distance user, you can add a feature for $3.13 per month for unlimited usage

Hardware Discount off MSRP
65% Discount for Voice and Data
50% Discount for Voice and or Data
61% Discount for accessories
All devices available for PFO's

Figure 2: Roaming Plan Description



ROGERS™

Roaming Plans

- Roaming package is stackable (see print screen below)
- Roaming plan is incorporated in each COB cellular device and ready for use when you enter a roaming zone
- Please follow the current approval process prior to your travel date to identify if roaming is requested for business or personal reasons. Mobility self-serve form can be found here: http://itservices.brampton.ca/HEAT/Default.aspx
- Detailed information on roaming plans and country zones are provided in the following pages

Following is a screen shot example of how the new stackable roaming plan works (applies to all countries) when you are on roaming mode:

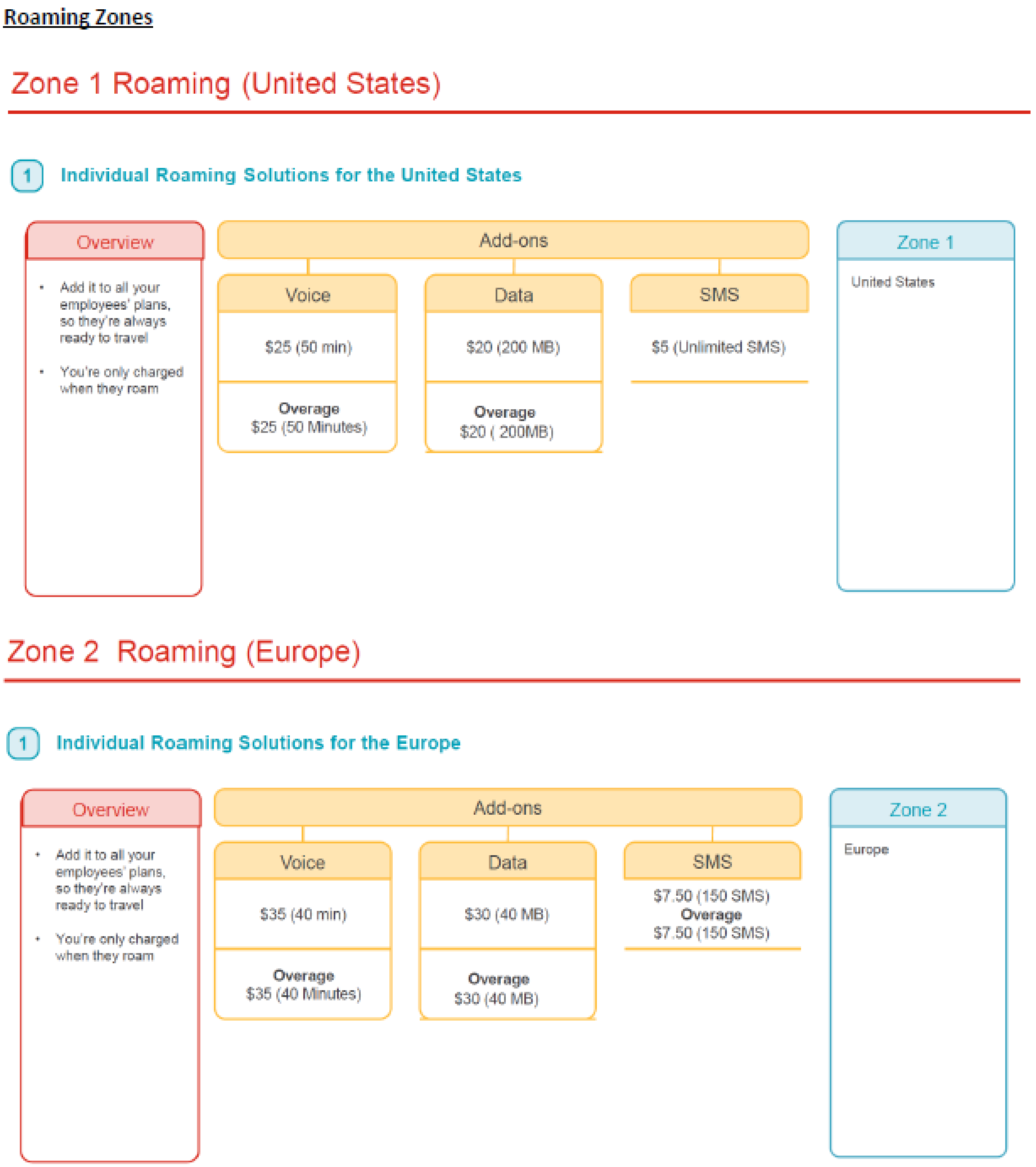
Zone 1 Roaming (United States)

1 Individual Roaming Solutions for the United States

- Add it to all your employees' plans, so they're always ready to travel
- You're only charged when they roam

Roaming plan is stackable which means if you exceed allotted data or voice, the overage kicks in. For example if data allotment is $20 for 200MB, as soon as usage reaches 200MB the next 200MB $20 is added automatically. This also applies to voice as well.

Figure 3: Roaming Rates for the Unites States and Europe



Roaming Zones

Zone 1 Roaming (United States)

1 **Individual Roaming Solutions for the United States**

Overview

- Add it to all your employees' plans, so they're always ready to travel
- You're only charged when they roam

Add-ons

Voice

$25 (50 min)

Overage
$25 (50 Minutes)

Data

$20 (200 MB)

Overage
$20 (200MB)

SMS

$5 (Unlimited SMS)

Zone 1

United States

Zone 2 Roaming (Europe)

1 **Individual Roaming Solutions for the Europe**

Overview

- Add it to all your employees' plans, so they're always ready to travel
- You're only charged when they roam

Add-ons

Voice

$35 (40 min)

Overage
$35 (40 Minutes)

Data

$30 (40 MB)

Overage
$30 (40 MB)

SMS

$7.50 (150 SMS)
Overage
$7.50 (150 SMS)

Zone 2

Europe