



Office of the Auditor General

Report on Audit Follow-ups

**Tabled at Audit Committee
May 29, 2019**



Office of the Auditor General

May 29, 2019

Mayor, Members of Audit Committee and Council,

I am pleased to present this report on follow-ups of audits carried out by the Office of the Auditor General of the City of Ottawa.

The report includes an overview and an executive summary for each of the follow-ups conducted.

Respectfully,

A handwritten signature in black ink that reads 'Ken Hughes'. The signature is written in a cursive style with a large initial 'K'.

Ken Hughes

Auditor General



Staff of the Office of the Auditor General

Ken Hughes

Sonia Brennan

Ed Miner

Chantal Amyot

Abhishek Gangwal

Sarah Parr

Louise Proulx

Margaret Sue

Nathan Sassi

Ines Santoro

Table of Contents

Progress toward improvement.....	1
Summary and assessment of overall progress made to date on audit recommendations	1
Executive summaries – Audit follow-ups	4
Follow-up to the 2015 Audit of Accounts Payable	5
Follow-up to the 2015 Audit of the Automated Meter Reading Project	10
Follow-up to the 2014 Audit of Winter Operations: Capacity Planning and Performance Measurement	12
Follow-up to the 2015 Audit of IT Governance	15
Follow-up to the 2015 Audit of IT Risk Management	22

Progress toward improvement

The Office of the Auditor General (OAG) conducts audit follow-ups two to three years after an audit is complete to afford management time to implement the recommendations. A follow-up may be conducted sooner if corrective action is complete. The OAG adheres to the best practices and professional standards of the international audit community by including the practice of audit follow-ups. The Audit Process includes the Planning Phase, the Fieldwork Phase, the Reporting Phase, and finally, the Follow-up Phase. In the follow-up, the OAG evaluates the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations. This evaluation ensures that the required measures, promised by management and approved by Council, have been implemented. Accordingly, the follow-ups in this report were conducted according to the OAG's 2017 and 2018 Work Plans.

The audit follow-ups contained in this report include:

- Audit of Accounts Payable
- Audit of the Automated Meter Reading Project
- Audit of Winter Operations: Capacity Planning and Performance Measurement
- Audit of IT Governance
- Audit of IT Risk Management
- Audit of Information Technology Security Incident Handling and Response (presented in camera)

As can be seen in the next section, it is clear from the results of these follow-ups that management is committed to the audit process.

Summary and assessment of overall progress made to date on audit recommendations

Audits are designed to improve management practices, enhance operational efficiency, identify possible economies and address a number of specific issues. The Follow-up Phase is designed to identify management's progress on the implementation of recommendations from the audit reports. This report is not intended to provide an assessment of each individual recommendation. Rather, it presents our overall evaluation of progress made to date across all completed audits. Should Council wish

to have a more detailed discussion of specific follow-ups, OAG staff are available to do so.

The table below summarizes our assessment of the status of completion of each recommendation for the above-noted audit follow-ups.

Table 1: Summary of status of completion of recommendations

Follow-up	Total	Complete	Partially complete	Not started	Unable to assess	No longer applicable
Accounts Payable	7	2	3	1	0	1
Automated Meter Reading Project	4	4	0	0	0	0
Winter Operations	20	17	3	0	0	0
IT Governance	9	4	5	0	0	0
IT Risk Management	8	0	7	0	1	0
IT Security Incident and Handling	11	6	4	0	1	0
Total	59	33	22	1	2	1
Percentage	100%	56%	37%	2%	3%	2%

We have categorized each of the audit follow-ups based upon the following criteria:

- **Solid progress** = 50% or more of the recommendations evaluated as ‘complete’.
- **Little or no progress** = 50% or more of the recommendations evaluated ‘not started’.
- **Gradual progress** = all others.

Solid progress:

- Audit of the Automated Meter Reading Project
- Audit of Winter Operations: Capacity Planning and Performance Measurement
- Audit of Information Technology Security Incident Handling and Response

Little or no progress:

- None

Gradual progress:

- Audit of Accounts Payable
- Audit of IT Governance
- Audit of IT Risk Management

Due to the importance of the outstanding issues on the IT-related follow-ups, the OAG will conduct further review to ensure full implementation of the recommendations. As a result of the annual work plan and/or Council requests, new audits in any of these areas may occur in the future.

Executive summaries – Audit follow-ups

The following section contains the executive summary of each of the audit follow-ups.

Follow-up to the 2015 Audit of Accounts Payable

The Follow-up to the 2015 Audit of Accounts Payable was included in the Auditor General's 2017 Audit Work Plan.

The original audit identified opportunities for the City to strengthen controls within Accounts Payable (AP) and use technology to increase the efficiency in processing invoices, maximizing cost savings and monitoring performance. The key findings raised in the original audit included:

- The roles, responsibilities and accountabilities of AP stakeholders are well defined, understood and supported by standards, procedures and tools.
- AP unit maintains a risk management process that aligns with the City's ERM Policy and allows for the ongoing identification, assessment, mitigation and monitoring of risks.
- Segregation of duties¹ (SOD) is necessary to mitigate the risk of potential errors and/or fraud. In situations where AP staff need system access above what has been assigned to their position, a review of potential SOD issues is required prior to granting enhanced access. While this process was verbally described, no documentation could be provided to demonstrate that the process was consistently and formally applied.
- Within SAP, there is a field that can be configured to enforce a check of duplicate invoices for all vendors prior to payment. This application control is configured as optional and not automatically applied as a mandatory check for all vendors. Reliance is placed on AP staff to manually select this field when they are creating a new vendor record or updating an existing vendor record. If the field is not selected when creating a vendor, there is a risk that duplicate payments can be processed for that vendor and manual compensating controls must be relied upon to detect duplicate payments.
- SAP contains key information on City vendors in "vendor master fields". Maintaining these fields is critical as sensitive information, such as banking information, is retained for vendors and forms the basis of payment. Access to modify this information requires strong controls to mitigate the risk of potential

¹ Segregation of Duties (SOD) is required for sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. (Source: aicpa.org)

fraud. When an employee creates a new vendor or updates information on an existing vendor in SAP, the change becomes active. No sensitive fields have been defined for which approval is required before the change becomes active in the system.

- Delays in reviewing and approving invoices cause delays in payment and missed discounts². AP implemented priority functionality within MarkView³ to notify users when potential discounts were coming due. While this functionality was in place, the notifications were not effective in distinguishing high priority invoices where an available discount was coming due or an invoice was about to be paid late. Clarifying the message in the notification would highlight those invoices and allow the business user to prioritize those invoices for immediate action.
- While the City is tracking the amount of missed discounts, it is not tracking penalties as a result of late payments.
- While AP performance monitoring has been established on a City-wide basis, limited analysis and reporting results are provided to business units on their individual results. There is an opportunity to leverage the tools and analysis within the AP unit to provide periodic reporting to business units on their specific results pertaining to discounts available but not taken, late payments, and average days taken to approve an invoice.
- Automation can be used to increase the efficiency and effectiveness of vendor invoice approval and processing. There are opportunities to better use technology to perform automated monitoring of discounts based on invoice receipt or acceptance date. Scanning technology can be configured to more accurately capture invoice information and decrease the amount of manual intervention required.

² Some vendor invoices contain an available discount if payment is made early or in advance of a defined date.

³ MarkView is the system that the City of Ottawa uses for automated invoice processing. This process receives an invoice from a vendor and reads key fields in the invoice for processing. Once processed, an AP clerk reviews the MarkView transaction details against the original invoice for completeness and accuracy prior to the verification and payment process.

Table 2: Summary of status of completion of recommendations

Recommendations	Total	Complete	Partially complete	Not started	No longer applicable
Number	7	2	3	1	1
Percentage	100%	29%	43%	14%	14%

Conclusion

Management has fully completed two out of six recommendations that are still applicable.

Follow up of one recommendation relating to required approval prior to vendor master field changes has not yet started. The City did not configure the sensitive vendor master fields in SAP because a new Source-to-Pay solution, expected to be implemented in 2020, will address this recommendation. As such, the risk that payments may be made before sensitive vendor master fields are adequately reviewed and approved remains.

The three partially completed recommendations are as follows: retention of documentation that shows SOD conflicts have been assessed and resolved prior to granting enhanced system access; processes to track and report on late penalties; and automated monitoring of potential discounts based on invoice receipt date. Additional information regarding the status of each partially completed recommendation is detailed below.

The original audit found that while the process of identifying potential SOD conflicts exists and that documentation should be available, no evidence could be provided to demonstrate that the process was consistently applied. As such, the audit recommended that the City retain documentation, which demonstrates that in cases where enhanced system access is granted, SOD conflicts have been assessed and resolved prior to approval. Our follow-up work found that while the requirement to retain documentation has been formalized, documentation has not been consistently kept for all instances where enhanced system access was granted.

The original audit also recommended that management establish a process to track and report on late penalties paid as a result of AP internal processes. Our follow-up work confirmed that while AP did set up a designated expense account in MarkView to track late penalties and interest, the responsibility is on the business user to identify the late

penalty on an invoice and code it to the expense account. AP was not able to provide evidence as to how or when business users were notified about this account and the requirement for them to code late fees or interest charges to this account.

Finally, the original audit recommended that the City leverage existing technology to ensure the efficiency and effectiveness of AP operations, including automating the monitoring of potential discounts based on invoice receipt date. The system enhancements for monitoring and analytics were deferred and will be addressed as part of the new Source-to-Pay solution.

One of the seven original recommendations is no longer applicable. When a solution was investigated, it was found that the current systems cannot provide more granular reporting on business unit results.

The Office of the Auditor General met with management regarding the partially completed recommendations, and they have indicated that they intend to complete the outstanding recommendations.

Recommendations and responses

Recommendation:

That AP formalize the requirement and steps to complete the semi-annual “duplicate invoice analysis” in a procedure document.

Management Response:

Management agrees with this recommendation.

The steps required to complete the semi-annual duplicate invoice analysis will be documented in a formal procedure by Q3 2019.

Recommendation:

Before the change to the Pcard transaction allocation is implemented, AP should notify Pcard users of the risk of duplicate invoices and their responsibility to implement a process to ensure that payments made in MarkView have not already been paid through a Pcard.

Management Response:

Management agrees with this recommendation.

Supply Services will include a reminder on the monthly statements sent to all cardholders of the risk of duplicate invoices and their responsibility to implement a process to ensure that payments made in MarkView have not already been paid through a Pcard. This will be completed in Q1 2019.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

Follow-up to the 2015 Audit of the Automated Meter Reading Project

The Follow-up to the 2015 Audit of the Automated Meter Reading (AMR) Project was included in the Auditor General's 2018 Audit Work Plan.

The key findings of the original 2015 audit included:

- The AMR project had a governance structure to ensure it was implemented and managed economically and efficiently. However, it lacked a steering committee; and a single business owner was not defined until over three years after the project was completed.
 - The project reported to Council semi-annually and informally to senior management; however, given the size and duration of the project, it was expected that a project steering committee (or similar) would have been established to provide guidance, direction and control.
- The project was adequately planned, implemented and managed economically and efficiently.
 - All 195,000 endpoints originally in-scope were successfully installed, including the 10,000 installs originally scoped out; and the project remained on schedule and budget.
- Most of the project's intended objectives, expected efficiencies, strategic goals and service improvements were achieved. However, cost-savings and the achievement of the project's strategic goals were not comprehensively tracked or reported on.
 - Although savings were realized as a result of a reduction in staff, the cost savings realized from the implementation of Advanced Metering Infrastructure (AMI) were not reported on.

Table 3: Summary of status of completion of recommendations

Recommendations	Total	Complete	Partially complete	Not started	No longer applicable
Number	4	4	0	0	0
Percentage	100%	100%	0%	0%	0%

Conclusion

Management has made significant progress, implementing all four recommendations. We suggest that in the future management include variable and fixed pricing in relevant contracts to incent contractors to carry out their duties in a manner consistent with City objectives.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

Follow-up to the 2014 Audit of Winter Operations: Capacity Planning and Performance Measurement

The Follow-up to the 2014 Audit of Winter Operations: Capacity Planning and Performance Measurement was included in the Auditor General's 2017 Audit Work Plan.

The key findings of the original 2014 audit included:

1. There was no documented process that considered resource capacity requirements for Winter Operations in the annual planning and/or budgetary cycle.
2. The existing Maintenance Quality Standards (MQS) for snow and ice control were adopted in May of 2003. Since that time they had not been systematically reviewed or assessed for financial impact.
3. The mix of internal and external service providers was primarily based on historical and/or legacy systems that were in place at the time of amalgamation (2001). Since that time there had not been a review to determine the optimal mix of internal and external service providers.
4. Public Works did not have a documented process to identify potential operational efficiencies.
5. When there was no requirement to apply abrasives or plow / clear snow, staff were assigned to miscellaneous duties. There was no documented list of tasks to be addressed on a priority basis and tasks could potentially have been provided more cost effectively by commercial sources.
6. All City and contracted roadway snow clearing vehicles were equipped with one of two task specific GPS. Management had not determined if the intended benefits of these investments in technology had been realized.
7. The City had a detailed communication plan for overnight parking bans. Management believed it would not be practical to implement a "rolling ban" for snow related overnight parking bans as is utilized in some municipalities.

Follow-up to the 2014 Audit of Winter Operations:
Capacity Planning and Performance Measurement

8. Monthly variance reporting included appropriate and relevant measures such as comparison of budgeted to actual and detailed costs by category. Reporting could have been enhanced by providing commentary on performance associated cost drivers.
9. The key performance indicators (KPIs) used in Winter Operations were the Council-approved Standards detailed in the MQS. These were not routinely reported to department management, Committee or Council. The KPI reporting did not include information available in the Ontario Municipal Benchmarking Initiative (OMBI) report.
10. Supervisors' reviews of snow clearing activities were largely unstructured and experience-based. There was no documented assurance that MQS were being applied consistently across the City or that standards were being met or overachieved.
11. The Standard Operating Procedure for salt deliveries allowed for acceptance of deliveries with a high variance and did not specify the number of times that random weighing should be performed. There was no monitoring to ensure portable weigh scales were used at every yard throughout the winter season and that contractors were not notified in advance. The amount of salt remaining in the spring of 2012, 2013 and 2014 was less than the amounts in inventory per SAP.
12. As of June 2015, 96% of workers and 95% of Supervisors in the Roads Services Branch had completed their Occupational Health and Safety Awareness Training. Public Works was in the process of assessing the risks of Winter Operations' occupations for the departmental Hazard Identification and Risk Assessment (HIRA).

Table 1: Summary of status of completion of recommendations

Recommendations	Total	Complete	Partially complete	Not started	No longer applicable
Number	20	17	3	0	0
Percentage	100%	85%	15%	0%	0%

Conclusion

Management has made good progress by completing 17 out of 20 recommendations.

Management also made significant progress in addressing the three partially complete recommendations. Management should continue to assess the costs, benefits and efficiencies of outsourcing resources on an ongoing basis in order to ensure the optimal mix of internal and external resources. Finally, the revised Roads Services dashboard, intended to enhance financial and KPI reporting, is expected to be implemented by the end of Q2 2019.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

Follow-up to the 2015 Audit of IT Governance

The Follow-up to the 2015 Audit of IT Governance was included in the Auditor General's 2018 Audit Work Plan.

The City of Ottawa's (the City's) IT Services Department (ITS) has principal responsibility for the deployment and maintenance of the IT resources used to deliver City services to people, businesses and visitors of Ottawa. ITS' net operating budget for 2013 was \$52.1 million, and it had a workforce of 352 full-time equivalents. ITS' 2013 capital budget was \$11.5 million. The City's governance structure, like those of other Ontario cities, facilitates the legislative process. It consists of several different but related bodies, namely City Council, Standing Committees, Advisory Committees and arms-length Agencies, Boards and Commissions ("ABCs"), and the regulatory tools that govern those Committees, such as the Procedure By-law, the Delegation of Authority By-law and the Public Notice By-law.

The governance structure is designed to enable formal, direct community input into decision-making through citizen's Advisory Committees and Standing Committee presentations to elected representatives. It also facilitates the legislative and governmental work of the elected officials through Standing Committees and City Council meetings. Information Technology (IT) Governance is a subset of the City's overall governance structure.

The original audit identified areas of improvement that were categorized into five overarching themes:

1. **Organizational and governance structures:** Guidance published by the Institute of Internal Auditors (IIA) states that "clear organizational structures, the operational nature of their components, how they communicate with each other, and the accountability protocols are important for the IT function to provide the required types and levels of services for the enterprise to achieve its objectives."

Specific findings from the original audit included:

- Lack of explicit documentation regarding how ITS supports the City in achieving its broad objectives;

- Risk that key items are not discussed at the Corporate Information Technology Management Team (CITMT¹) as the meetings do not follow a formal agenda;
- The IT Governance Committee² is not supported by formal Terms of Reference and therefore there is no formally approved document to describe its purpose and structure; and
- The Individual Contribution Agreements³ (ICAs) lack “measurable” objectives (i.e. successfully implementing projects on time or within budget). Such objectives are considered good practice in serving to reinforce accountabilities of ITS personnel, including the Chief Information Officer (CIO).

2. **Executive leadership and support:** Strong tone at the top and executive leadership plays an important role in ensuring alignment between IT and the wider organizational objectives. This means that there is a strong vision among senior management and the executive regarding the strategic importance and potential of the IT function. There are several elements which enable strong leadership and executive support and which we expected to find over the course of our audit.

Specific findings from the original audit included:

- High turnover rate of the Chief Information Officer (CIO);
- Lack of communication of ITS’ role in achieving the City’s strategic objectives; and
- Lack of established performance indicators related to ITS’ strategic value.

3. **Strategic and operational planning:** A strategic plan, which lays out organizational dependencies on IT as well as ITS’ role in achieving the organization’s strategic objectives, is a crucial component of effective IT

¹ CITMT was dismantled subsequent to the original audit.

² IT Governance Committee was discontinued subsequent to the original audit.

³ On December 05, 2017 a City Employee Communications Memo stated: “As announced at the City Manager forums last year, the City has moved away from the formal ICA process towards a dynamic practice focused on regular manager/supervisor and employee check-in conversations throughout the year”. The new process is referred to as “Performance Management”.

Governance. Leading practices also emphasize the need for alignment between ITS' tactical operating plan and the corporate strategic plan.

Specific findings from the original audit included:

- Lack of explicit linkage and common terminology between the Strategic Plan and the IT projects described in the Technology Roadmap;
- The Strategic Plan does not clearly define ITS' role and responsibilities in achieving strategic objectives nor does it identify the City's IT-related dependencies;
- We did not identify more evidence of how the City considered and accounted for current and planned IT capacity within the Technology; and
- Lack of use of performance indicators and related measures – the current suite of performance measures were found to be insufficient as they focus only on basic operational aspects of the IT function (e.g. “down time”) as well as the basic measures associated with IT projects.

4. **Service delivery and measurement:** As identified in GTAG 17⁴, an effective performance management framework “...captures the right quantitative and qualitative data to enable proactive measurement, analysis, and transparency further assures sound IT governance.”

Specific findings from the original audit included:

- Stakeholders are not clear about how IT costs contribute to the City's strategic objectives; and
- ITS does not effectively measure its value either in terms of contributions to strategic goals or the business benefits associated with IT projects.

5. **IT organization and risk management:** In evaluating the IT organization's risk management practices, the original audit expected to find three key elements. Firstly, the original audit expected there to be standard IT hardware, software, and service procurement policies, procedures, and controls in place. Secondly, that risks be managed effectively in relation to meeting the City's needs, security, and

⁴ Institute of Internal Auditors - Global Technology Audit Guide (GTAG) 17: Auditing IT Governance - <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/pages/gtag17.aspx>

compliance requirements. Finally, GTAG 17 indicates an expectation that data is standardized and easily shared across applications and the IT infrastructure.

Specific findings from the original audit included:

- Lack of documentation supporting the identification and assessment (likelihood and impact) of risks within ITS.
- Lack of guidance within the ITS Risk Management Policy as to how higher priority IT risks should be communicated up to the City’s Corporate Risk Committee. It was also unclear how corporate risks are cascaded down from the corporate level to ITS, resulting in unclear alignment between ITS risks and City-wide/corporate risk.

To address the areas of improvement above, the original Audit of IT Governance provided nine recommendations for implementation by the City of Ottawa. The follow-up to the 2015 Audit of IT Governance assessed the status of completion for each recommendation, results of which are summarized in Table 1 below. Details on the assessment are included in the detailed report.

Table 4: Summary of status of completion of recommendations

Recommendations	Total	Complete	Partially complete	Unable to assess
Number	9	4	5	0
Percentage	100%	44%	56%	0%

The recommendations found to be partially completed included:

- *That CITMT be supported by formal agendas and the IT Governance Committee, to the extent it continues to act in a formal role, and that it be supported by a formal Terms of Reference, which documents the Committee’s purpose and structure.* The CITMT and IT Governance Committee were discontinued subsequent to the original audit, replaced by the Business Technology Committee and the Senior Management Committee respectively. We recognize the update of governance committees since the original audit, and the existence of formal terms of reference and standing agendas are in place for the new Committees; however, we noted that the City’s current IT risk policies and processes are inconsistent regarding roles, responsibilities and authorities related to approval requirements for exemptions / exceptions from standard procedures (which impacts the effectiveness of governance mechanisms).
- *That going forward, the process to develop objectives for purposes of the CIO’s ICA is reviewed to better reflect objectives that are measurable.* We noted that the CIO has completed his latest ICA and performance objectives and that these were based on outlined Objectives and Key Results (OKRs); however, additional objectives could be considered for assessing performance of the CIO such as the resolution of specific OKRs in ITS IT Strategic Work Plan associated with significant recommendations from the original IT Governance, Risk Management and Remote Access audits (outlined in Section 8 of the ITS IT Strategic Work Plan).
- *That management expedite the recruitment of an appropriately qualified and experienced CIO. Further, that they review and confirm expectations and related practices concerning the CIO to ensure alignment with leading practices whereby the IT function is viewed, empowered and supported as a strategic enabler.* We noted in the original audit (March 2015) that the “extent of turnover at the CIO position has been substantial. The departure of the recently hired CIO in December 2013 meant that, since March 2004, there have been 8 individuals either in the CIO position or acting in that role, including 5 since June 2012.”⁵ The CIO job description did not require the candidate to explicitly be an “experienced CIO”, and we noted that the CIO subsequently left the City in January 2019.

⁵ City of Ottawa, Office of the Auditor General, Audit of IT Governance – March 2015, page 7

- *That management develop an effective CIO succession plan to be implemented once a new CIO is retained.* We noted that a formal, documented succession plan did not exist for the CIO position.
- *That the ITS Risk Management Policy include guidance on how higher priority IT risks should be communicated up to the City's Corporate Risk Committee⁶.* Further, ITS should work with City Staff to develop guidance around expectations for the communication of corporate risks down to ITS. ITS should also develop or obtain formal documentation which describes the identification and assessment of IT risks within the Department. We recognize the update of governance committees since the original audit, and the existence of formal terms of reference and standing agendas are in place; however, we noted that the City's current IT risk policies and processes are inconsistent regarding roles, responsibilities and authorities related to approval requirements for exemptions / exceptions from standard procedures, limiting the effectiveness of governance and oversight for these exemptions.

Conclusion

Although management has shown some progress towards the implementation of recommendations from the Audit of IT Governance, the Office of the Auditor General (OAG) noted that a number of key areas remain in need of remediation. Specifically, five of nine recommendations were assessed only as partially complete.

We noted that ITS has established a visible linkage between IT Services and the City's broad objectives. This has been via two new initiatives, a new Intake process and ITS' Strategic Work Plan that establishes a framework for how ITS will plan and work from 2018 to 2020. Both of these initiatives were observed to have 'client-centric' focuses that link business needs with ITS services. We noted that the ITS scorecard has been discontinued, and ITS uses a client dashboard to display metrics including service requests per department, intake projects, department activity, and that this dashboard is in a pilot phase before its broader roll-out. Objectives and Key Results metrics were also introduced, and we observed evidence demonstrating that these metrics have been scored and monitored monthly as suggested in the ITS Strategic Work Plan – Section 14.1.2.

⁶ The Corporate Risk Management Committee was dismantled subsequent to the original audit.

We recognize that governance committees have been updated since the original audit, and that formal terms of reference and standing agendas are in place; however, we noted some inconsistencies within the City's current IT risk policies and processes regarding roles, responsibilities and authorities related to approval requirements for exemptions / exceptions from standard procedures.

We noted that the City is once again faced with the challenge of recruiting and establishing a new CIO. In the interim, there is increased risk that the effectiveness of IT governance may be significantly impaired. Additionally, the Department has failed to adequately resolve a number of audit findings in a timely basis as far back as 2015, .

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

Follow-up to the 2015 Audit of IT Risk Management

The Follow-up to the 2015 Audit of IT Risk Management was included in the Auditor General's 2018 Audit Work Plan.

Throughout the City, IT-based solutions and innovations have supported the achievement of a variety of operational and strategic objectives. The role of technology is expected to continue a steep growth pattern as new and innovative solutions are developed. However, while there are opportunities for IT to support the City's strategic objectives, there are a variety of traditional and emerging IT risks that must be considered and effectively managed at the highest level.

For an organization of the complexity and size of the City of Ottawa, the breadth and depth of potential IT-related risks is significant. Whether it is maintaining operational or administrative capabilities, protecting valuable or sensitive assets, supporting compliance or enabling achievement of business or strategic imperatives, there is an inherent risk relating to IT in nearly every City activity or function. As such, while there is obviously a technical element of IT risk, business managers from across the City are ultimately the most important stakeholders in the management of IT risks.

The management of IT risks is supported through a number of policies, processes and practices at both an enterprise-wide and at a more granular level (e.g. at the IT project level or incident response level). At the enterprise level, IT-related risks are explicitly captured within the ERM Framework. While Information Technology Services (ITS) is the single most significant source of IT risks, IT risks were identified by 65 per cent of all departments in 2014.

ITS plays an important role in the management of IT risks at the project and systems level. In addition to providing training/awareness sessions related to IT risks, ITS is responsible for developing IT-related policies and guidance to support the management of IT risks.

ITS has a formal and broad responsibility for the management of IT risks, however, there are independent IT groups that serve in a few departments where one or more business applications or systems that, while often connected to enterprise architecture, operate fully or in part, autonomously from ITS. These include Transit Services, Traffic Operation Branch, Drinking Water Services Branch and Wastewater Services Branch.

The original audit identified areas of improvement that were categorized into three audit objectives:

1. **Assess if IT Risk Management Governance at the City effectively supports management of the City's IT-related risks**

Specific findings from the original audit included:

- Lack of an Information Technology Risk Management (ITRM) Framework including a comprehensive Governance component and clear and consistent responsibilities and accountabilities for City executives and management;
- The decentralized method of prioritizing, selecting and funding IT initiatives may result in approved projects that are not aligned with corporate priorities, and significant risk was identified that high priority IT risks are not being adequately addressed on a timely basis where funding is not readily available to the business owner;
- The Corporate Information Technology Management Team (CITMT¹) authority to discharge its responsibility for recommending a corporate IT plan that is reflective of risk-based IT priorities across the City is hindered by the IT project model as well as the City's existing capability to identify and prioritize City-wide IT risks; and
- The CIO's authority and ability to influence and manage City IT resources is limited as staff responsible for IT in various departments and agencies (e.g. Ottawa Public Health, Transit, Water, Wastewater, etc.) are not accountable to the CIO and lines of authority are not always clear, and the CIO's authorities and responsibilities for City-wide IT risks are not formally defined.

2. **Assess if the City's IT Risk Management Framework of policies, practices and procedures are adequately designed and aligned with the City's ERM Framework**

Specific findings from the original audit included:

- Lack of a comprehensive IT Risk Management Framework that serves to bridge the gap between ERM and more granular ITRM.

¹ CITMT was dismantled subsequent to the original audit.

- There are many deficiencies in the documentation to support the identification, assessment and mitigation of IT risks. The design effectiveness of the existing ITRM framework is reduced by: insufficient documented and approved ITRM framework with a supporting policy and procedures suite, insufficient processes for the identification and assessment of City-wide IT risks, weaknesses in challenge mechanisms for assessment of proposed/possible corrective measures, insufficient training of ITS staff, IT professionals outside of ITS and others who are non-IT professionals yet are tasked with performing IT risk assessment, undocumented IT risk universe that would serve to support oversight and inform decision-makers, and incompleteness of Business Technology Plan including how the plan is based on mitigating the highest risks/priorities as well as related timelines, costs and sources of financing.
- The low maturity level of most City departments for ITRM and the broad and technical nature of IT risks, procedures and guidance at both the corporate and departmental level are not sufficient to ensure that the identification, evaluation, communication, mitigation, and monitoring of the most important IT risks is consistent, appropriate and timely. In addition, IT issues and priorities that are critical to City-wide objectives do not necessarily rise to the top.

3. **Assess if the City's IT Risk Management policies, practices and procedures are effectively supporting the identification, evaluation, mitigation and monitoring of IT risks across the City**

Specific findings from the original audit included:

- There is neither the culture nor capacity to support a complete and holistic view of IT risks and the effective management of these risks;
- Outputs may not have been subject to sufficient analysis, consideration and challenge by people with appropriate and sufficient skill sets/competencies to effectively perform this function;
- Some IT-related issues may not be appropriately identified, assessed and subsequently escalated to both inform (awareness) and mitigate (plans and funding);
- It is not clear if all risks related to aging infrastructure, data storage, network capabilities, etc. have been identified; and

- There is not always a linkage between the identification of a critical risk with the provision of sufficient resources allocated for effective mitigation.

To address the areas of improvement above, the original Audit of IT Risk Management provided eight recommendations for implementation by the City of Ottawa. The follow-up to the 2015 Audit of IT Risk Management assessed the status of completion for each recommendation, results of which are summarized in Table 1 below. Details on the assessment are included in the detailed report.

Table 5: Summary of status of completion of recommendations

Recommendations	Total	Complete	Partially complete	Unable to assess
Number	8	0	7	1
Percentage	100%	0%	88%	12%

The recommendations found to be partially completed included:

- *That the City Manager develops a robust Governance component of an ITRM Framework which:*
 - *Is aligned to the ERM Framework and includes governance capable of supporting a mature risk culture embedded in an ITRM Framework with a supporting policy suite and processes.* We observed that policies for governance have been aligned with the goals of the ERM framework, but the annual risk validation process, which is a key process in the ITRM Framework, was being developed at the time of the audit.
 - *Includes clearly defined roles, responsibilities, and authorities of City Executives and Management to establish clear delineation of those Responsible, Accountable, Consulted and Informed for effectiveness of the ITRM.* Roles and responsibilities have become more clearly defined with the introduction of the ITRM Framework, however we noted that the City’s current IT risk policies and processes are inconsistent regarding approval requirements for exemptions or exceptions from standard procedures (which affects roles, responsibilities and also governance and oversight of IT risks). We further identified that Business Support Services resources lack

technology understanding and formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessments.

- *Clearly establishes the basis for a corporate risk culture, including risk tolerance and risk appetite guidelines.* The City has made improvements by establishing its risk appetite and tolerance guidelines, including the collection of 53 service area risks, the introduction of a formalized risk exemption process, and an annual risk validation process is under development.
- *Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are considered for inclusion in the Annual Corporate IT Plan based on risk/priority, regardless of whether there is pre-approved funding identified.* We have noted that the ITS plan is focused on capital expenditure as well as the development and/or update of key processes, and funding is linked with Objectives and Key Results. However, the City of Ottawa's funding models have not facilitated the mitigation of operational IT risks related to the 2015 Audit of IT Security Incident Handling & Response finding [REDACTED], indicating funding for operational IT risks may not have kept pace.
- *That the City Manager and City Treasurer undertake an assessment of IT spending to explore alternative funding models which will provide better alignment between mitigation of prioritized City-wide IT risks and funds available/provided and provide long term savings through improved, targeted IT spending.* The City has established new funding models to allow the funding for unacceptable IT risks. However, the City of Ottawa's funding models have not facilitated the mitigation of operational IT risks related to the 2015 Audit of IT Security Incident Handling & Response finding [REDACTED], indicating funding for operational IT risks may not have kept pace.
- *That the City Manager take steps to strengthen the effective authority of CITMT including expanding reviews to include all City-wide IT risks and proposed/recommended mitigation strategies.* The City has established the Technology Security Risk Management Team as an oversight body for risk mitigation and decision making. We noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions / exceptions from standard procedures which affects governance and oversight of IT risks.

- *That the City Manager take steps to strengthen and confirm the role, responsibility and accountability of the Director, ITS and CIO position including consideration of alignment with the best practices identified in the ISACA RISK-IT Framework as well as functional reporting of all City departments and agencies to the CIO for all IT matters.* The City has updated its Information Security Policy and prepared an Information Technology Risk Framework outlining the roles and responsibilities of key positions with respect to its IT risks. We noted that these practices are aligned with the ISACA RISK-IT Framework, and require the completion of the annual risk validation process currently under development as a key part of tracking and managing IT risks.
- *That the CIO develop a robust ITRM Framework which:*
 - *Is aligned to the ERM Framework.* We noted that an ITRM Framework has been developed and that alignment is in place.
 - *Incorporates the recommended Governance component of an ITRM framework (Refer to Recommendation #1).* As above, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions or exceptions from standard procedures, which affects governance and oversight of IT risks.
 - *Includes clearly defined roles, responsibilities, and authorities for all City employees involved in ITRM.* As above, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions or exceptions from standard procedures (which affects governance and oversight of IT risks).
 - *Incorporates a well-documented audit universe/inventory and a risk register.* An IT inventory universe has not been completed that would serve to support identification of potential IT risks. A risk register exists and a recent quarterly review was performed.
 - *Incorporates a well-developed challenge mechanism conducted by trained and qualified IT professionals.* At the time of the assessment, we observed two mechanisms that are involved in the IT risks challenge function: the exemption/exception process which was observed to have inconsistent approval requirements in City practices, and the annual risk validation process which was in development and we noted that resources assigned to this process required additional support in terms of training, experience and time available to the establishment of this process.

- *Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are communicated to Senior Management in a comprehensive and effective manner.* An operational risk register is in place, which is used to communicate risks using a dashboard. Business Support Services personnel are assigned as the departmental contact of all risk management activities, and were noted to lack technology understanding and/or formal risk training to assist them with identifying potential IT risks and participating in IT risk assessment.
- *That the CIO, in conjunction with the development of the ITRM Framework, develop a supporting policy and procedure suite that:*
 - *Incorporates all required processes for completion of the ITRM Framework including a robust challenge mechanism.* As above, we noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework, and we noted that the exemption/exception process was observed to have inconsistent approval requirements.
 - *Specifies the skill sets and training required of those responsible for completion of departmental components of the ITRM documents.* We did not observe evidence that skill sets and training specifications for departmental components of the ITRM documents were specified.
 - *Embeds the strengthened role of the CIO.* We noted that significant progress was made to further define the CIO role since the previous audit. However, the role of the CIO in the City's current IT risk policies and processes is inconsistent regarding approval requirements for exemptions or exceptions from standard procedures.
- *That all City departments, with direction and support from ITS:*
 - *Ensure departmental staff preparing ITRM documents have the requisite skills and tools to adequately and completely prepare all required ITRM documents.* As above, Business Support Services personnel are assigned as the departmental contact of all risk management activities, and were noted to lack technology understanding and/or formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessment. Additionally, we noted that the approach to perform a quick review process to capture existing IT risks using existing TRA information may not properly identify all IT risks at the City requiring assessment, and additional ITS

resources to perform risk assessment and related mitigation planning and monitoring activities may be required.

- *Develop departmental processes, which ensure that all components of the business line are included in required ITRM documents.* We noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework.
- *Develop review and challenge mechanisms designed to ensure that all ITRM documents are completed to an appropriate level of granularity which fully facilitates the understanding of IT risks, impact and the management and tracking of strategies related to the mitigation of IT risks.* As above, we noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework, and we noted that the exemption/exception process was observed to have inconsistent approval requirements.

The recommendations that were unable to be assessed included:

- *That the CIO as well as and City-wide managers continue to improve the identification and assessment of IT and related mitigation strategies, while using the ITRM Framework recommended in Recommendations 1 and 2.* The ITRM framework was established in 2018, which includes an annual requirement for review and update. Since the annual review deadline had not yet passed at the time of the assessment, and the annual review had not yet occurred, we were unable to assess this recommendation.

Conclusion

Management has shown minimal progress towards the implementation of recommendations from the Audit of IT Risk Management. Specifically, seven of eight recommendations were assessed only as partially complete, and the remaining one recommendation could not be assessed through this follow-up.

While management responses stated that recommendations in many cases were completed based upon the implementation of the City's IT Risk Management Framework, and various processes e.g. risk assessment process, risk exemption process, annual risk validation process, etc., the auditors have not been provided sufficient evidence that these have been successfully and/or correctly implemented.

Based on the processes documented by the City as well as discussions with ITS staff, a key component to understanding the risk posture of the City involves an annual risk validation process. This process is not fully developed or documented; however, it is widely used to identify risks within the City. Given the scope and complexity of the risk management initiatives, the City should consider whether resource requirements should be further allocated to perform IT risk management functions.

Additionally, the City's Business Support Service (BSS) representatives are responsible for identifying and communicating potential IT risks and participating in risk assessments and in many cases are referred to by staff as "risk practitioners". We noted that these resources also lacked technology understanding and/or formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessment.

While the Threat and Risk Assessment (TRA) process in place is designed to identify IT risks based on new projects, initiatives or changes in technology, it does not address the identification of IT risks for existing technologies at the City that have not been subject to new projects, initiatives or changes.

For the identification of IT risks for existing technology at the City, ITS completed a pilot for 2 of the 53 City service areas to determine the effort required to capture IT risks. Following the pilot, it was decided by management that proceeding to capture IT risks by service area through risk information sessions was deemed not to be worth the level of effort. Instead, an approach with a quick review process using existing TRA information was performed to produce service area risk profiles which would then be subject to annual technology risk validations (this validation process was still under development at the time of the follow-up audit). The audit team was not provided with listings of systems where TRA's had been performed.

The audit notes that this approach, coupled with an incomplete IT risk universe, may not properly identify all IT risks at the City requiring assessment, and additional ITS resources to perform risk assessment and related mitigation planning and monitoring activities may be required (for example to operationalize the annual risk validation process). Given the City's organizational size and complexity, and since the full risk management program has not yet been fully operationalized, it is unlikely that a full appreciation and understanding of the City's IT risk universe is possible with the current resources available, restricting the City's ability to identify and prioritize mitigation of its IT risks on a timely basis and be strategically aligned to add organizational value.

We also noted that the City's current IT risk policies and processes are inconsistent regarding roles, responsibilities and authorities related to approval requirements for exemptions / exceptions from standard procedures. This inconsistency in practices also affects governance and oversight of IT risks, impacting six of eight previously identified recommendations. The *IT Risk Management Framework* (dated January 18, 2018), the *Information Security Policy* (dated July 16, 2018) and the *Technical Security Risk Exemption Process* (dated September 7, 2018) indicate conflicting information for approvals and authorities related to approving exemptions / exceptions from standard procedures. Depending on the document referenced, either the SLT, the TSRM, or the CIO and Department Head are required to approve [high] risk exemptions / exceptions. In practice, we observed that exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM, impairing the effectiveness of oversight of these governance bodies. Additionally, we noted that the exemption, which allowed the storage of personally identifiable information in the US, was both submitted and approved by the City CIO, and no City policy or process indicates whether this is an acceptable practice. We encourage the City to explore potential issues associated with this practice.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.