



**Office of the Auditor General**

**Follow-up to the 2015 Audit of IT Governance**

**Tabled at Audit Committee**

**May 29, 2019**

**Table of Contents**

Executive summary ..... 1

    Conclusion ..... 6

    Acknowledgement..... 7

Detailed report – Assessment of implementation status ..... 8

## Executive summary

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 (CITMT<sup>1</sup>) as the meetings do not follow a formal agenda;
- The IT Governance Committee<sup>2</sup> 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 Agreements<sup>3</sup> (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.

---

<sup>1</sup> CITMT was dismantled subsequent to the original audit.

<sup>2</sup> IT Governance Committee was discontinued subsequent to the original audit.

<sup>3</sup> 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”.

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 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 17<sup>4</sup>, 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.

---

<sup>4</sup> 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>

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 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 1: Summary of status of completion of recommendations

<b>Recommendations</b>	<b>Total</b>	<b>Complete</b>	<b>Partially complete</b>	<b>Unable to assess</b>
<b>Number</b>	9	4	5	0
<b>Percentage</b>	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.”<sup>5</sup> 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.

---

<sup>5</sup> 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 Committee<sup>6</sup>.* 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.

---

<sup>6</sup> 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.

## Detailed report – Assessment of implementation status

To complete the assessment, the auditors reviewed key City policy and process documents, including the Intake Process v1.5, IT Project Intake Overview-v3\_FINAL, ITS Strategic Work Plan 2018-2020, ITS Dashboard Snapshot, MEMO – New Intake Process for IT Projects BN, Software Rationalization Policy Final Review.

The auditors also conducted numerous interviews with various ITS information security team members including the City CIO, and the Manager of Technology Solutions.

Following this, five projects were selected and assessed to determine whether they were managed according to ITS' intake process. These projects were the only large projects to have been processed through the new intake process. The projects selected for review were:

- Contact Centre Technology Renewal Project;
- Microsoft M365 Proposal;
- Public Wi-Fi service;
- SAP Hana Database Upgrade; and
- Land Management Solution.

The following information outlines management's assessment of the implementation status of each recommendation as of August 2018 and the Office of the Auditor General's (OAG) assessment as of December 2018.

**Recommendation #1**

Table 2: Status

Management update	OAG assessment
Complete	Complete

**Audit recommendation:**

That ITS develop documentation that clearly establishes the linkage between IT Services and the City’s broad objectives to support governance bodies and others in the promotion and monitoring of alignment of the City’s needs with IT Services. This linkage should be tracked and monitored using the ITS Scorecard.

**Original management response:**

Management agrees with this recommendation.

The Business Technology Plan replaced the previous Technology Roadmap and was approved by the IT Sub-Committee in November of 2013. The Business Technology Plan includes key IT projects that directly support strategic objectives in the City Strategic Plan and articulates the role of ITS in supporting those projects to achieve their stated objectives. The Business Technology Plan initiatives are tracked and monitored on a monthly basis using the ITS Scorecard.

**Management update:**

**July 2016**

Management considers this recommendation complete. The Business Technology Plan and the ITS Scorecard no longer exist; however, in Q4 of 2015 the IT project intake model was further evolved and approved by senior management. The current model uses a funnel/gating process with identified checkpoints to manage the life of a project and includes a monthly project dashboard and health check.

The Corporate Project Management methodology has been adopted and the Corporate Business Case template is the standard intake tool to support decision-making. Every department wishing to initiate an IT project must first complete a Business Case, and clearly indicate how their project aligns to the City Strategic Plan and/or corporate priorities.

Additionally, clients must develop relevant performance measures that demonstrate the business value associated with their projects. Client departments are responsible for creating, tracking, and reporting on their performance measures.

The current IT Governance structure composed of the Business Technology Committee (replaces the former Corporate IT Management Team, 'CITMT') and the Senior Leadership Team is responsible for prioritizing and monitoring the overall status of IT projects.

Please note that over the next six months, ITS will work in collaboration with business areas to ensure that the governance structure aligns with changes in corporate direction and the organizational re-alignment. Client feedback will be incorporated into any changes going forward.

### **August 31, 2018**

In the recent organizational realignment, Information Technology Services (ITS) transitioned to structured functional branches and positioned itself to align its priorities with the City's strategic objectives.

Focusing efforts on client needs, ITS has collaborated with other City departments to identify linkages, determine business priorities, resource requirements, and governance oversight.

The ITS Intake Process, approved by the Senior Leadership Team in 2016, focuses on client needs once a business need is identified through ITS' Technology Solutions branch, whose functions also include gathering business requirements, annual IT planning and prioritization, and IT project intake governance.

Identified large projects now require review by members of the Senior Leadership Team (including the sponsor department's General Manager (GM), the Chief Information Officer, the City Treasurer and GM of the Corporate Services Department, and the GM of the Service Innovation and Performance Department), followed by confirmation of the organization's investment in the initiative.

Upon approval, both small and large IT projects proceed to the project life cycle for implementation, tracking and monitoring. All large and small projects are identified on a real-time IT Client Dashboard, which is being piloted with Business Support Services branches and IT Services to support information sharing and transparency around IT-related initiatives.

**OAG assessment:**

The actions as described in the management update were assessed as complete.

We noted that ITS has established visible linkages between IT Services and the City's broad objectives, both through the ITS Intake process and the 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.

The ITS Intake Process collaboratively includes staff members from outside of ITS such as the City Treasurer and GM of the Corporate Services Department, and the GM of the Service Innovation and Performance Department.

The ITS Strategic Work Plan identifies "Client-Centric" as a foundational principle, with the expectation that "processes, products, and services should be delivered in a way that maintains the experience of the client in mind – whether that is a line of business partner, or ultimately the resident who is impacted by a service."<sup>7</sup>

We noted that while the ITS scorecard has been discontinued, ITS now uses the ITS client dashboard to track and monitor a number of general 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 (OKRs) metrics were also introduced in the ITS Strategic Work Plan, dated February 2018, where each branch is responsible for developing key results that align to the IT Services objectives and directly support the strategic direction of the corporation. We observed that OKRs were established in the ITS Strategic Work Plan at the Branch Leadership Team and Staff levels, and additionally observed evidence demonstrating that OKR metrics have been scored and monitored monthly.

---

<sup>7</sup> ITS Strategic Work Plan 2018-2020 – Pg. 9

**Recommendation #2**

Table 3: Status

Management update	OAG assessment
Complete	Partially complete

**Audit recommendation:**

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.

**Original management response:**

Management agrees with this recommendation.

Formal agendas for the CITMT meetings are part of the governance process and have been consistently in place since January 16, 2014. As a result of this recommendation, Management will undertake a further review of the agenda format to ensure standing items, such as Confirmation of Minutes and Roundtable, are addressed at each meeting.

In April of 2014, the IT Governance Committee was replaced by the Senior Management Committee (SMC) to further align the IT governance model with the existing City corporate governance structure. The Terms of Reference for CITMT were developed in 2013 and further revised in April 2014 to reflect the change in reporting structure from the IT Governance Committee to SMC.

**Management update:**

**July 2016**

Management considers this recommendation complete. The Business Technology Committee (BTC) was established in Q1 2016, which replaced the Corporate IT Management Team. As with CITMT, all BTC agendas and meeting materials are posted on a wiki. Meeting agendas and related materials are posted one week in advance of each meeting and meeting minutes are posted within one week following each meeting.

Regular standing items for each agenda have been established to ensure meeting minutes are approved, and action logs are used to identify and track outstanding work items.

The Terms of Reference were refreshed when the Business Technology Committee was launched, and will be reviewed every six months as will the committee membership.

### **August 31, 2018**

The ITS governance model aligns with the existing City corporate governance structure and ITS Intake Process. Large projects (defined as highly complex, multi-year planning and implementation, and resource intensive solutions) require approval from the GM of Corporate Services and City Treasurer (CSD), the GM of Service Innovation and Performance (SIPD) and the GM of the sponsoring client department (as per Recommendation 1 response update). Approval is sought through a detailed briefing note via e-mail from the Manager of Technology Solutions, which is also supported by the CIO, the business owner / project sponsor and the ITS Business Analyst.

The GMs may determine that the proposed item is not a priority for the organization; in this case, the project will not proceed, their decision will be documented, and no further action will be required. If the GMs determine that this item is a priority for the organization and that a detailed business case should be developed to support this direction, the IT Business Analyst will work with the client to co-author the business case.

Most large projects are not anticipated to require the endorsement of all members of the Senior Leadership Team; however, if the GMs of CSD and SIPD deem it necessary to obtain full SLT approval, it will be sought. SLT decisions and approvals are also documented.

Lastly, a Technology Risk Management (TRM) governance body has been established that includes the CIO, the City Clerk and Solicitor and the GM of Corporate Services and City Treasurer, should the risk level of a project require an elevated level of acceptance. The Technology Security branch and Technical Architects facilitate in identifying when this governance body should be engaged (further details provided in Recommendation 9 response update).

**OAG assessment:**

The actions as described in the management update were assessed as partially complete.

We recognize the update of governance committees since the original audit, and the existence of formal terms of reference and standing agendas for the Business Technology Committee, documenting the Committee's purpose and structure.

However, during our review of the documentation associated with the follow-up audit of IT Risk management, 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 also affects governance and oversight of IT risks.

*IT Risk Management Framework* (dated January 18, 2018) indicates:

- the TSRM is responsible for recommending risk treatment and exceptions to SLT
- the Senior Leadership Team is responsible for approving any exceptions to policy or procedures

*Information Security Policy* (dated July 16, 2018) indicates approval for exemptions to Information Security Policies must be approved by the CIO and the Department Head requesting the exemption (or their delegate).

The *Technical Security Risk Exemption Process* (dated September 7, 2018) indicates that approval is required commensurate with the risk assessed, where:

- Low Risk: Approved or denied by the Program Manager (PM), Technology Security (TS).
- Medium Risk: Approved or denied by the Chief Information Officer (CIO), Information Technology Services.
- High Risk: Approved or denied by the Technology Security Risk Management (TSRM) team.

As the above demonstrates, 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 the TSRM and/or the SLT. 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; no policy or process indicates whether this is an acceptable practice, and we encourage the City to explore potential issues associated with this practice.

**Impact:**

A lack of appropriate governance could limit executive management's accurate visibility of significant IT-related risks and the success with which the City is addressing them. Proper governance practices also promote a risk-aware culture, and facilitate risk-aware decision making. Improper governance practices can result in erroneous or delayed identification of critical IT risks to the City, and could lead to risk-taking without a full understanding of the potential nature or severity of consequences.

**Recommendation #3**

Table 4: Status

Management update	OAG assessment
Complete	Partially complete

**Audit recommendation:**

That going forward, the process to develop objectives for purposes of the CIO’s ICA is reviewed to better reflect objectives that are measurable.

**Original management response:**

Management agrees with this recommendation. The performance expectations and objectives of the CIO will be documented in an annual work plan to support the job description deliverables, Business Technology Plan, City Strategic Plan and departmental operational plans. The CIO’s performance on the objectives outlined in the work plan will be reviewed and documented via the annual ICA process with the Deputy City Manager, City Operations.

**Management update:**

**July 2016**

Management considers this recommendation complete. The CIO completed his 2015 ICA and the 2016 performance objectives as per the corporate performance management process and timelines.

A new CIO was appointed by the City Manager as part of the corporate realignment on July 13, 2016. The 2016 performance objectives previously identified will be reviewed by the new CIO and the General Manager, Corporate Services and City Treasurer and will be documented in the on-line PDP tool.

**August 31, 2018**

The CIO completed his 2017 ICA and 2018 performance objectives, which are driven by the “Objectives and Key Results (OKRs)” Framework (see Recommendation 6 and 7 response updates). The CIO shared the ICA and performance objectives with the ITS Management team.

**OAG assessment:**

The actions as described in the management update were assessed as partially complete.

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, good practice suggests that a number of further objectives could be considered for assessing performance of the CIO. We noted for example, that at the time of this audit, a number of critical findings identified in three separate audits dating back to 2015 were either partially completed or unable to assess. Many of these findings hold significant risk to the City.

The ITS IT Strategic Work Plan specifically noted the IT Governance and IT Risk Management audits, where specific OKRs were assigned to each audit findings, which could be tied to the CIO's performance assessment. [REDACTED]<sup>8</sup>. We also noted that 360-style reviews of the CIO's performance (for meeting the expectations of a leader as an example), are not part of the CIO's overall performance criteria. Although the CIO has focused on many key strategic points to further the City's IT organization, it is important that items requiring remediation be a continued focus. The City should consider revisiting the metrics for the CIO to be measured based on a number of key indicators including (but not limited to): strategic leadership, people management, mentoring, personal development, training and overall annual initiatives such as hiring new staff to reinforce areas of concern, planned and executed updates to IT infrastructure, as well as compliance and controls areas (security, policies and procedures, technical training, budgets) which may provide some supplemental metrics suitable for complementing CIO performance reviews.

**Impact:**

A lack of complete performance indicators could limit a full understanding of the achievements and unresolved challenges as they relate to meeting specific business objectives, and to the overall health of the ITS department, staff support, and other important areas.

---

<sup>8</sup> [REDACTED]

**Recommendation #4**

Table 5: Status

Management update	OAG assessment
Complete	Partially complete

**Audit recommendation:**

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.

**Original management response:**

Management agrees with this recommendation. The recruitment of the next CIO is currently in progress and is scheduled to be completed by the end of Q3 2014. Management agrees that the CIO position is a critical position within the organization and is a strategic enabler to assist the City in achieving its strategic goals. The expectations regarding the role and its deliverables will be set during the recruitment process and further outlined in the letter of offer to be sent to the successful candidate. As part of the on-boarding process, the Deputy City Manager, City Operations and the new CIO will review the work plan referenced in the management response to Recommendation 3 and will discuss overall performance expectations.

**Management update:**

**July 2016**

Management considers this recommendation complete. As indicated above, a new CIO was appointed by the City Manager as part of the corporate realignment on July 13, 2016. As per the regular PDP process, the new CIO’s 2016 performance deliverables will be reviewed and approved by the General Manager, Corporate Services and City Treasurer and documented in the on-line PDP tool.

**August 31, 2018**

A new CIO was appointed by the City Manager as part of the corporate realignment on July 13, 2016. As per the regular Performance Review process, the new CIO's performance deliverables will be reviewed and approved by the General Manager, Corporate Services and City Treasurer.

**OAG assessment:**

The actions as described in the management update were assessed as partially complete.

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.”<sup>9</sup>

The official City of Ottawa job description for the CIO required a minimum of 10 years of related experience, including experience in the information technology field. It does not appear that the job description adequately set the bar for the minimum expectations for the audit recommendation “appropriately qualified and experienced CIO”, since the description did not require that the candidate explicitly had previous CIO experience.

We understand that the hired CIO had limited previous IT related experience as well as a computer engineering degree. We noted that the CIO additionally spent the previous 6 years with the City as Director Economic Development and Innovation, a role and position which permitted good insight into the technology and related services in use at the City.

The CIO is responsible for setting and aligning the IT strategy with the broader business strategy. It is also important to note that the CIO role at the City is strategic and hands-on, including vetting and approving large capital IT projects, and assessing risk and approving exceptions to standard policy.

---

<sup>9</sup> City of Ottawa, Office of the Auditor General, Audit of IT Governance – March 2015, page 7

A successful CIO should demonstrate strong leadership, capable of inspiring and leading IT managers, analysts, and developers while bridging technology with business strategies. This should be coupled with a strong understanding of technology given the responsibility of minimizing cost while maximizing the results of technology. As an executive, these qualities often come from prior experience in a previous CIO role, VP in a technology role, IT director, where candidates require not only a strong business understanding but also a solid IT background to be successful.

We noted that the CIO hired in July 2016 subsequently left the City in January 2019, and was replaced on an interim basis by an internal candidate, who was not identified in a formal CIO succession plan (see Recommendation #5).

**Impact:**

As identified in the original audit report, “without a qualified and experienced CIO, there is an increased risk that the effectiveness of IT governance within any organization as large and complex as the City of Ottawa would be considerably impaired”.<sup>10</sup>

---

<sup>10</sup> Office of the Auditor General Audit of IT Governance – March 12, 2015, page 7

**Recommendation #5**

Table 6: Status

Management update	OAG assessment
Complete	Partially complete

**Audit recommendation:**

That management develop an effective CIO succession plan to be implemented once a new CIO is retained.

**Original management response:**

Management agrees with this recommendation. As part of the corporate succession planning strategic initiative, all critical roles in the ITS department have been identified and succession plans are currently in development / implementation as part of the departmental workforce planning. The succession plan for the CIO will be reviewed by the Deputy City Manager, City Operations and the new CIO by Q1 of 2015 and development plans will be established with the potential successors.

**Management update:**

**July 2016**

Management considers this recommendation partially complete. In January 2016 the ITS Department was realigned to have an Operational Branch and a Strategic Branch. This resulted in the creation of two new Senior Manager roles to oversee these respective areas. These two leadership positions have been identified as successor roles for the CIO.

The General Manager, Corporate Services and City Treasurer will be reviewing the succession plan for the CIO by the end of Q4 2016 following which, development plans will be established for potential successors.

**August 31, 2018**

Since the 2016 re-organization, seven manager positions have been created that report directly to the CIO. Through a formal succession planning process, working with the HR service partner, all seven positions are being provided the necessary opportunity and experience to step into an acting CIO role. The expectation is that all of them would be part of the internal pool of candidates for a permanent CIO replacement.

Individual Contribution Agreement (ICAs) discussions for 2018 will further confirm interest from each manager and appropriate development plans will be put in place.

**OAG assessment:**

The actions as described in the management update were assessed as partially complete.

We noted that at the time of the audit, a formal, documented succession plan did not exist for the City of Ottawa's CIO position.

A review of the current experience of two individuals within the City's ITS group identified as potential successors for the CIO indicated that neither resource had the experience to meet the City's requirements to replace the CIO on a permanent basis.

**Impact:**

An individual placed in the IT leadership role lacking the correct experience, either from a technical and/or leadership perspective, could lead to the development of a strategy that does not fully align with the City's overall needs, risks or future state. As a result, this could lead to unsuccessful technology deployments, cost overruns, financial losses and may impact the City's ability to obtain efficiency opportunities as stipulated in the ITS Strategic Work Plan.

**Recommendation #6**

Table 7: Status

Management update	OAG assessment
Complete	Complete

**Audit recommendation:**

That management ensure that the city’s strategic objectives, as reflected in the Technology Roadmap, articulate the linkage to key IT projects. ITS’ role in achieving strategic objectives, performance metrics, and IT-related dependencies should also be reflected.

**Original management response:**

Management agrees with this recommendation. The Business Technology Plan, which replaced the previous Technology Roadmap and was approved by Council’s IT Sub-Committee in November of 2013, is currently where these relationships are captured. Management will examine opportunities to further align the Business Technology Plan with key initiatives and objectives outlined in the City Strategic Plan to further articulate the role of ITS in supporting these projects and will continue to monitor ITS capacity through the annual review of the Business Technology Plan. Business benefits and associated key performance measures are the joint responsibility of ITS and client departments leveraging the technology to achieve their business outcomes.

**Management update:**

**July 2016**

Management considers this recommendation complete. As referenced in the response to Recommendation 1, the Business Technology Plan no longer exists. Departments must now use the Corporate Business Case to indicate how their projects align with the City Strategic Plan and/or corporate priorities.

Client departments are responsible for creating, tracking, and reporting on their performance measures, and demonstrating the business value associated with their IT projects. ITS’ role in supporting the technology components of each client project are articulated in every business case.

Please note that over the next six months, ITS will work in collaboration with business areas to ensure that the governance structure aligns with changes in corporate direction and the organizational re-alignment. Client feedback will be incorporated into any changes going forward.

### **August 31, 2018**

As referenced in the management response to Recommendation 1, the Technology Roadmap no longer exists. In 2017, Information Technology Services (ITS) developed a three-year Strategic Work Plan and a high-level summary. Unlike past strategic work planning exercises that have resulted in a fixed set of major initiatives, this Strategic Work Plan establishes a framework for how ITS will plan and work for the next three years.

The ITS Strategic Work Plan is organized into four overarching objectives; objectives that ensure ITS is positioned as the organization's technology partner of choice. By 2020, ITS will:

- i. Provide clients with access to tools and information anytime, anywhere, from any device;
- ii. Promote operational efficiency, enabling response to both rapid growth and rapid change;
- iii. Develop and support leading edge technology tools and practices that support the business priorities of the corporation; and
- iv. Provide clients with secure, modern, reliable infrastructure and tools to support their business needs.

The achievement of these objectives will be monitored using a well-established framework of 'Objectives and Key Results (OKRs).' Each branch is responsible for developing key results that align to the IT Services objectives and directly support the strategic direction of the corporation. The three-year Strategic Work Plan is refreshed every year, with additional attention given to aligning new objectives and key results to new and/or updated corporate strategic objectives with IT implications.

**OAG assessment:**

The actions as described in the management update were assessed as complete.

We noted that ITS has established visible linkages between IT Services and the City's broad objectives, both through the ITS Intake process and the 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.

The ITS Intake Process collaboratively includes staff members from outside of ITS such as the City Treasurer and GM of the Corporate Services Department, and the GM of the Service Innovation and Performance Department.

The ITS Strategic Work Plan identifies "Client-Centric" as a foundational principle, with the expectation that "processes, products, and services should be delivered in a way that maintains the experience of the client in mind – whether that is a line of business partner, or ultimately the resident who is impacted by a service."<sup>11</sup>

We noted that while the ITS scorecard has been discontinued, ITS now uses the ITS client dashboard to track and monitor a number of general 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 (OKRs) metrics were also introduced in the ITS Strategic Work Plan, dated February 2018, where each branch is responsible for developing key results that align to the IT Services objectives and directly support the strategic direction of the corporation. We observed that OKRs were established in the ITS Strategic Work Plan at the Branch Leadership Team and Staff levels, and additionally observed evidence demonstrating that OKR metrics have been scored and monitored monthly.

---

<sup>11</sup> ITS Strategic Work Plan 2018-2020 – Pg. 9

**Recommendation #7**

Table 8: Status

Management update	OAG assessment
Complete	Complete

**Audit recommendation:**

That ITS continue to work toward developing additional KPIs related to their performance and to the business benefits associated with IT projects.

**Original management response:**

Management agrees with this recommendation. It is the client department’s responsibility to report on the business benefits and associated key performance measures. As part of the CITMT planning process for identifying departmental and/or corporate initiatives requiring ITS resources, client departments are required to complete a corporate business case which specifies the business value and any expected performance measures, such as the estimated return on investment (ROI) and planned project timelines. Client departments are expected to further refine the project details and deliverables in their project charter documents, and are responsible for tracking and realizing the benefits associated with their IT projects.

**Management update:**

**July 2016**

Management considers this recommendation complete. As referenced in the responses to Recommendations 1 and 6, clients must identify relevant performance measures for their IT projects in their business cases. Client departments are responsible for creating, tracking, and reporting on their performance measures, and demonstrating the business value associated with their IT projects.

Please note that over the next six months, ITS will work in collaboration with business areas to ensure that the governance structure aligns with changes in corporate direction and the organizational re-alignment. Client feedback will be incorporated into any changes going forward.

### **August 31, 2018**

As per Recommendation 6 response update, the achievement of ITS strategic objectives will be monitored using a well-established framework of 'Objectives and Key Results (OKRs)'.

OKRs are set annually, and progress against each OKR is reviewed quarterly by the ITS management team. When developing and refining annual OKRs, ITS staff and managers actively consult with industry and public sector peers to keep informed of best practices and new technology developments to validate the areas in which ITS is dedicating valuable resources.

As well, operational work planning tied to activities occurs at the branch level and is monitored by each branch manager.

In addition to operational service levels and performance measures, IT Services has put in place an online training forum for all staff to continuously improve and modernize their skill sets in order to better support new and upcoming business technology needs. This training tool has been well received and is widely used to support industry certifications and cross-training efforts.

### **OAG assessment:**

The actions as described in the management update were assessed as complete.

We noted Objectives and Key Results (OKRs) metrics were introduced in the ITS Strategic Work Plan, dated February 2018, where each branch is responsible for developing key results that align to the IT Services objectives and directly support the strategic direction of the corporation. We observed that OKRs were established in the ITS Strategic Work Plan at the Branch Leadership Team and Staff levels, and additionally observed evidence demonstrating that OKR metrics have been scored and monitored monthly.

**Recommendation #8**

Table 9: Status

Management update	OAG assessment
Complete	Complete

**Audit recommendation:**

In developing the performance measures referenced in Recommendation 6, that ITS consider, among others, specific measures that will support a better understanding of how IT expenditures are contributing to the City’s strategic objectives and identify ITS’ capacity to conduct projects.

**Original management response:**

Management agrees with this recommendation. As part of the CITMT planning process, departments are required to outline the business value associated with their proposed IT projects and demonstrate clear alignment to the strategic initiatives and objectives identified in the City Strategic Plan. Direct alignment to Council-approved priorities is a main criterion for IT project and resource approval via the IT governance process. As referenced in the management response to Recommendation 7, departments are required to specify the business value and expected deliverables and performance measures within a corporate business case document and subsequent project management documents, such as charters. Departments are responsible for tracking their project deliverables and measuring outcomes. Management, as part of the IT governance process, will summarize and monitor all measures emanating from IT projects identified in the approved Business Technology Plan and will explore suitable measures to demonstrate ITS’ contribution of expenditures and resources to the City’s strategic objectives.

**Management update:**

**July 2016**

Management considers this recommendation complete. As referenced in Recommendation 6, the onus is on each department to demonstrate the business value, the expected outcomes/deliverables, and the associated performance measures for their IT projects. All project costs, including those from ITS and the business area, as well as the cost of any ongoing support and maintenance, are to be documented in the Corporate Business Case. ITS capacity constraints and proposed mitigations are discussed at BTC on a monthly basis.

**August 31, 2018**

As per Recommendation 6 response update, the ITS Strategic Work Plan is organized into four overarching objectives; objectives that ensure ITS is positioned as the organization's technology partner of choice and is a highly mature IT practice. Specifically, objective two states that by 2020, ITS will promote operational efficiency, enabling response to both rapid growth and rapid change.

ITS is currently embodying this objective through the SAP HANA upgrade, in making the City of Ottawa perhaps the first Canadian public sector organization to use an in-house HANA implementation/integration team. ITS is able to better utilize funds provided by developing and growing in-house resources.

As well, ITS is developing its Platform Alignment Strategy. The consolidation of core technologies and simplification of business processes for both ITS and the City will achieve the following benefits: consistent license management; ease of integrations; enhanced security; improved application reliability and availability; optimized server utilization; simplified infrastructure management; reduced maintenance costs; reduced cost, time, and risk with application upgrades; reduced Total Cost of Ownership; response time improvement to client requests; shared/larger technical resource pool for support and development; simpler technical architecture; advanced data analytics capabilities; consistent user experience; reduced application downtime; seamless customer interactions; and shortened cycle from business idea to technology implementation.

**OAG assessment:**

The actions as described in the management update were assessed as complete.

We recognize the City has made operational efficiency an objective in the ITS Strategic Work Plan, and the Platform Alignment Strategy for consolidation of core technologies may permit the potential realization of benefits to the City.

We noted that there are many Branch Key Results that include efficiencies within an objective such as “Drive efficiency and innovation by leveraging Mobile Device Management to its fullest potential”, and observed individual OKRs that identified expenditure metrics to support a better understanding/linkage of how these specific activities are impacting IT expenditures, linked to the City’s strategic objectives.

**Recommendation #9**

Table 10: Status

Management update	OAG assessment
Complete	Partially complete

**Audit recommendation:**

That the ITS Risk Management Policy include guidance on how higher priority IT risks should be communicated up to the City’s Corporate Risk Committee. 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.

**Original management response:**

Management agrees with this recommendation. The ITS Information Risk Management Policy is used to manage information risk according to its criticality and importance to the City. The Policy is directly linked to the City’s Enhanced Risk Management framework and identifies that the Director, ITS and CIO has overall responsibility for risk management activities within the department, including ensuring that higher priority IT risks are communicated appropriately. Further, as part of the City’s Enhanced Risk Management program, each department follows the corporately approved process to identify, assess and mitigate risk. Each department submits a corporate risk profile and register on an annual basis that identifies and provides an assessment of the risks within a department. These risk profiles, which capture higher priority IT risks, are assessed by Corporate Business Services and reported to the Corporate Risk Management Steering Committee and Senior and Executive Management. Corporate risks are communicated down to the ITS department to ensure alignment.

**Management update:**

**July 2016**

Management considers this recommendation complete. The ITS Information Risk Management Policy is used to manage information risk according to its criticality and importance to the City.

The policy is directly linked to the City's Enhanced Risk Management framework and identifies that the CIO has overall responsibility for risk management activities within the department, including ensuring that higher priority IT risks are communicated appropriately. Furthermore, through the City's Enhanced Risk Management Program each department must identify, assess, and mitigate technology risks in each of their Risk Profiles. When a department identifies a technology risk, there is a process in place by which ITS is notified in order to review/assess the risk and follow-up with the business if necessary.

In addition, an IT Risk Management Strategy and Roadmap is currently being developed and is pending funding in 2017 and beyond. The goal of this strategy is to evolve the current security state into a corporate service that is scaled to manage IT risks at a level acceptable to the City. The strategy will address key areas of governance, policies, authority, and accountability, and will ensure that the City is prepared to meet the challenge of an ever-changing threat landscape.

### **August 31, 2018**

IT risk management practices have been enhanced as a result of the audit response project work related to the 2015 IT Risk Management Audit.

The ITS Information Risk Management Policy referred to in the July 2016 update, is the newly updated and approved Information Security Policy (ISP). The ISP mandates IT risk management practices for the City, which is fulfilled by way of the IT Risk Management Framework (ITRM).

This approved Framework aligns to the City's Enterprise Risk Management (ERM) practices, which includes the reporting, escalation and communication of risks to senior leadership. As well, ITS has an established governance structure, supporting risk management processes (including escalation) and a Risk Register solution in place. This Register tracks both technology and technology security risks including mitigation actions and their follow-up.

As per the Framework, the CIO is responsible/accountable for all technical and technical security risks at the City as well as the Framework itself. While the service area owns and is responsible/accountable for their data, the security of the data and complete technical environment is owned by the CIO. At the CIO's discretion, the exemption may be escalated to the City's Technology Risk Management governance structure, which consists of the City Solicitor, City Treasurer and CIO.

**OAG assessment:**

The actions as described in the management update were assessed as partially complete.

We noted that a documented IT Risk Management Framework (ITRM) outlines the overall governance model related to risk management and is in alignment with the City's ERM framework.

However, during our review of the documentation associated with the follow-up audit of IT Risk management, 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 also affects governance and oversight of IT risks).

*IT Risk Management Framework* (dated January 18, 2018) indicates:

- the TSRM is responsible for recommending risk treatment and exceptions to SLT
- the Senior Leadership Team is responsible for approving any exceptions to policy or procedures

*Information Security Policy* (dated July 16, 2018) indicates approval for exemptions to Information Security Policies must be approved by the CIO and the Department Head requesting the exemption (or their delegate).

The *Technical Security Risk Exemption Process* (dated September 7, 2018) indicates that approval is required commensurate with the risk assessed, where:

- Low Risk: Approved or denied by the Program Manager (PM), Technology Security (TS).
- Medium Risk: Approved or denied by the Chief Information Officer (CIO), Information Technology Services.
- High Risk: Approved or denied by the Technology Security Risk Management (TSRM) team.

As the above demonstrates, 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 the TSRM and/or the SLT. 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; no policy or process indicates whether this is an acceptable practice, and we encourage the City to explore potential issues associated with this practice.

**Impact:**

A lack of appropriate governance could limit executive management's accurate visibility of significant IT-related risks and the success with which the City is addressing them. Proper governance practices also promote a risk-aware culture, and facilitate risk-aware decision making. Improper governance practices can result in erroneous or delayed identification of critical IT risks to the City, and could lead to risk-taking without a full understanding of the potential nature or severity of consequences.

Table 11: Status legend

<b>Status</b>	<b>Definition</b>
<b>Not started</b>	No significant progress has been made. Generating informal plans is regarded as insignificant progress.
<b>Partially complete</b>	The City has begun implementation; however, it is not yet complete.
<b>Complete</b>	Action is complete, and/or structures and processes are operating as intended and implemented fully in all intended areas of the City.
<b>Unable to assess</b>	Action is not currently taking place; however, remains applicable.