Office of the Auditor General

Follow-up to the 2015 Audit of IT Governance

Tabled at Audit Committee
April 27, 2021

Table of Contents

Executive summary

The Follow-up to the 2015 Audit of IT Governance was included in the Auditor General's 2020 Audit Work Plan.

The previous follow-up Audit of IT Governance tabled at Audit Committee May 29, 2019 identified that four of the nine recommendations from the 2015 audit were complete and five were partially complete. As a result, the follow-up was subsequently included in the Auditor General's 2020 Work Plan, to re-visit the remaining five recommendations.

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[1]) as the meetings do not follow a formal agenda;
   - The IT Governance Committee[2] is not supported by formal Terms of Reference and therefore there is no formally approved document to describe its purpose and structure; and

[1] CITMT was dismantled subsequent to the original audit.

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

- The Individual Contribution Agreements[3] (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 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

[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".

- Lack of use of performance indicators and related measures – the current suite of performance measures was 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[4], 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 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.

[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

To address the areas of improvement above, the original Audit of IT Governance provided nine recommendations for implementation by the City of Ottawa. The 2018 and 2020 follow-ups to the 2015 Audit of IT Governance have assessed the status of completion for each open 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

Recommendation	Status as at December 2018	Management status as at August 2020	OAG status as at November 2020
#1	Complete	-	-
#2	Partially complete	Complete	Complete
#3	Partially complete	Complete	Complete
#4	Partially complete	Complete	Complete
#5	Partially complete	Partially complete	Partially complete
#6	Complete	-	-
#7	Complete	-	-
#8	Partially complete	Complete	Complete
#9	Complete	-	-
Total	**4 Complete (44.4%)** **5 Partially complete (55.6%)**	**4 Complete (80%)** **1 Partially complete (20%)**	**4 Complete (80%)** **1 Partially complete (20%)**

Conclusion

Since our previous follow-up in 2018, management has completed four recommendations. These are in relation to governance and roles and responsibilities in relation to the Technology Security Risk Management (TSRM) body; performance objectives for the CIO; the recruitment of an appropriately qualified CIO; and how risks are communicated and escalated.

One recommendation remains outstanding. This is in relation to succession planning for the role of CIO. Management stated that a succession plan is in place for the CIO, however there was limited documentation available in relation to the plan. Additionally, the potential individuals identified were expected to have individual development plans, however they were not available at the time of the audit.

Acknowledgement

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

Detailed report – Assessment of implementation status

The following information outlines management's assessment of the implementation status of each recommendation as of August 2020 and the Office of the Auditor General's (OAG) assessment as of October 2020.

Recommendation #2

Table 2: Status

Management update	OAG assessment
Complete	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 (ToR) 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).

August 2020

To address inconsistencies raised by the OAG in the follow-up report, ITS updated the following documents in December 2019 to align roles and responsibilities across policies: The Information Security Policy (ISP), the IT Risk Management Framework (ITRM) and, the Enterprise Risk Management Policy (ERMP). This includes criteria and examples on approval authority and the addition of an annual risk validation process. Additionally, a Terms of Reference was developed for, and approved by, the Technology Security Risk Management (TSRM) governance team on December 13, 2019. The above-mentioned documents were communicated to stakeholders in December 2019.

OAG assessment:

Upon reviewing the provided documentation, it was noted that the Technology Security Risk Management (TSRM) governance body will support business decisions around technology security risks. This is composed of Legal, GM Public Works and the GM of Innovative Client Services who all have voting rights. The CIO is included as an advisory member.

The TSRM Terms of Reference was reviewed and it was noted that there is no formalized schedule for the frequency of meetings, which is defined in the ToR as “Meetings will be scheduled and held as required”.

Additional documentation was provided detailing the “Foundation and Roles for TSRM” dated October 16, 2019. This includes TSRM responsibilities, meeting procedures and the ‘exemptions process’. A TSRM channel in Microsoft Teams has been created and is now used for risk discussions. We note that this is a relatively informal communication channel for risk discussions, however the use of Teams was agreed and approved by the TSRM, and has benefits given the need for remote working as a result of the COVID-19 pandemic.

Recommendation #3

Table 3: Status

Management update	OAG assessment
Complete	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.

August 2020

Performance objectives for the CIO position continue to be set and measured annually based on outlined objectives and key results (OKRs) and, the ITS Work Plan.

Development objectives for director-level positions at the City, including the CIO, are reviewed annually as part of the corporate Individual Development Plan process. The acting CIO and the General Manager, Innovative Client Services reviewed progress against development objectives as part of the Individual Development Plan (IDP) process in 2020.

Director-level positions (including the CIO) also participate in corporate leadership development programs such as the Leadership Circle, which includes peer and staff review and coaching.

OAG assessment:

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

Objectives and Key Results were provided and reviewed. The CIO informed OAG that he provides his work plan to various departments for input. Timelines are defined by working with departments to develop roadmaps. Priorities are set in agreement with the General Manager of Innovative Client Services.

It was noted that the 2020 OKRs spreadsheet contains 662 named objectives, with 638 named KRs. The objectives range from modernization programs, training and development of City of Ottawa staff to maintaining and enhancing database security.

Recommendation #4

Table 4: Status

Management update	OAG assessment
Complete	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 complete.

OAG has noted that there have been a number of changes within the department. This includes the appointment in 2019 of a General Manager to the new Innovative Client Services (ICS) department. There is also now a new role created and filled since February 2020 entitled 'Chief Information Security and Digital Risk Officer (CISO)' to develop and mature the security practices within the City.

While noted that the existing CIO is in role in an 'acting' capacity, the CIO has been with ITS for over 20 years and OAG was informed that this appointment is planned to be extended due to the ongoing pandemic situation. On this basis OAG believe it would not be of benefit at this time to appoint a new permanent CIO to the role and the recommendation be marked as complete.

Recommendation #5

Table 5: Status

Management update	OAG assessment
Partially 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.

August 2020

Innovative Client Services identified potential successors to the CIO position in February 2020 through the Corporate Succession Management Program.

The GM, Innovative Client Services will work with the acting CIO and the identified employees to create Individual Development Plans to prepare them for the role of CIO. These plans will be completed by Q4 2020.

OAG assessment:

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

The City is leveraging the Succession Management toolkit as part of the work to develop identified individuals. As the acting CIO is planning to remain in role for the immediate future, this will help to facilitate a transition to the identified candidate. OAG enquired of Management for the additional documentation in relation to a specific CIO succession plan, as only the standard City of Ottawa succession plan template was initially provided. A spreadsheet entitled "Succession Plans_RCFS IT" was subsequently provided with a last updated date of 6th November 2020. Upon review it was noted that five individuals are listed including the existing CIO. Four of the individuals have a readiness noted of 3-5 years. A number of other fields within the spreadsheet were empty.

Individual Development Plans for those personnel who have been identified as potential successors were also not available at the time of the audit.

Recommendation #9

Table 6: Status

Management update	OAG assessment
Complete	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.

August 2020

Implementation of this recommendation is complete.

See response and supporting documents provided for Recommendation #2.

OAG assessment:

The actions as described in the management update under Recommendation #2 and #9 were assessed as 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.

Upon reviewing the provided documentation, it was noted that the Technology Security Risk Management (TSRM) governance body will support business decisions around technology security risks. This is composed of Legal, GM Public Works and the GM of Innovative Client Services who all have voting rights. The CIO is included as an advisory member.

Additional documentation was provided detailing the "Foundation and Roles for TSRM" dated October 16, 2019. This includes TSRM responsibilities, meeting procedures and the 'exemptions process'. A TSRM channel in Microsoft Teams has been created for members of the TSRM governance body and is now used for risk discussions and to capture and record approvals.

Table 7: Status legend

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