Office of the Auditor General

Follow-up to the 2015 Follow-up Audit of IT Risk Management

Tabled at Audit Committee
April 27, 2021

Table of Contents

Executive summary

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

The previous follow-up Audit of IT Risk Management tabled at Audit Committee May 29, 2019 identified that seven of the eight recommendations from the 2015 audit were partially complete and one was unable to be assessed at the time. As a result, the follow-up was subsequently included in the Auditor General's 2020 Work Plan, to re-visit the eight recommendations.

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 (CITMT[1]) 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

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

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.
- 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. All eight findings were subsequently assessed as part of this audit. 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 asserted status August 2020	OAG assessment status as at November 2020
#1	Partially complete	Complete	Complete
#2	Partially complete	Complete	Complete
#3	Partially complete	Complete	Complete
#4	Partially complete	Complete	Complete
#5	Partially complete	Complete	Complete
#6	Partially complete	Complete	Complete
#7	Partially complete	Complete	Complete
#8	Unable to Assess	Complete	Complete
Total	**7 Partially Complete (88%)** **1 Unable to Assess**	**8 Complete** **(100%)**	**8 Complete** **(100%)**

Conclusion

Since our previous follow-up in 2018, management has completed all eight of the recommendations. The TSRM process is now v2.0 with additional improvements now in place and better alignment to the Enterprise Risk Management process. The Annual IT Risk Management Validation process has also been conducted to perform additional verification on the ‘High rated’ IT risks.

While we recognize that all areas where previous observations were raised have been completed by Management, there were minor observations where controls in the area could be further improved, namely formalization of risk management decisions and further reconciliation of risk mitigation strategies.

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

To complete the assessment, the auditors reviewed key City policy and process documents, including the ITRM Framework 2.0, risk exemption process, ITRM Annual Risk Validation process, Information Security Policy, etc.

The auditors also conducted interviews with various ITS information security team members including the City CIO, Manager of Technology Solutions, Chief Information Security/Digital Risk Officer.

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 November 2020.

Recommendation #1

Table 2: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

That the City Manager develops a robust Governance component of an ITRM Framework which:

- Is aligned to the ERM Framework.
- Includes clearly defined roles, responsibilities, and authorities of City Executives and Management.
- Clearly establishes the basis for a corporate risk culture, including risk tolerance and risk appetite guidelines.
- 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.

Original management response:

Management agrees with this recommendation.

The City Manager will work with ITS and the Corporate Programs and Business Services department to develop a robust Governance component of an ITRM framework. Work done to implement this recommendation will be completed in conjunction with work being done to implement Recommendation 5. This recommendation will be complete by Q4 2016.

August 2020 management update:

To address inconsistencies raised by the OAG in the follow-up report, ITS has updated the Information Security Policy (ISP), the IT Risk Management Framework (ITRM) and Enterprise Risk Management Policy (ERMP) to align roles and responsibilities across policies. This includes criteria and examples on approval authority and the addition of an annual risk validation process.

The Technical Security Risk Management (TSRM) governance team was established in July 2017 to oversee the ITRM.

The Annual Risk Validation Process was completed City-wide in January 2020. All risk assessments and validation work were conducted by trained Technology Security team members. The Technology Security Branch has invested in training and certifications for staff.

A new Chief Information Security / Digital Risk Officer (CISO) position has been added to the IT management team, reporting directly to the General Manager of the Innovative Client Services department. This position is responsible for maturing the current security program as well as developing a strategic approach for continuous improvement.

OAG assessment:

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

OAG was informed that ERM is managed to a certain level of risk appetite. Low risks are addressed when the threat risk landscape changes. Changes to risks were made as part of the COVID pandemic impact.

We have noted that the City has produced an updated IT Risk Management Framework document v2.0 on December 13, 2019. The updated document is now more aligned to the Enterprise Risk Management Policy (ERMP) and contains Roles and Responsibilities for the Technology Security Risk Management Team (TSRM); CIO; Department Leadership Team; Technology Security Branch (TSB) and Business Support Services.

Risk scores are calculated using the 5x5 Risk Mapping which aligns to the ERMP. It was noted that Low Risks (scores between 1-4) are not tracked. Risk scores of 5-12 can be approved by the CIO and 15-25 scores need to be approved by the TSRM.

For activities related to mitigations, tickets are raised through Marval ticket request system and assigned to relevant area. The business planning aspect is included in the overall process and items needing attention are identified as priority item.

As per the Enterprise Risk Framework, all departments are responsible for managing their respective risks, including those in the IT Risk Register and Dashboard.

OAG was informed that the Innovative Client Services Department Manager, Business Support Services manages Enterprise risks in a spreadsheet, which is fed by the IT Plan. It was noted that the reconciliation of the mitigation strategies appears to be limited and Management should consider further reconciliation activities to provide further enhancements in relation to this.

Recommendation #2

Table 3: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

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.

Original management response:

Management agrees with this recommendation.

The City Manager, CIO and City Treasurer will work to identify and implement a budgeting/funding model that will allow for the funding of risk items that are deemed unacceptable. This funding model will form a part of the ITRM framework referenced in Recommendation 5. This recommendation will be complete by Q2 2016.

2018 management update:

The City Treasurer and the Chief Information Officer (CIO) have worked to identify a budgeting/funding model that will allow for the funding of risk items that are deemed unacceptable.

The model includes:

- An increased capital budget for Information Technology Services (ITS) for the lifecycle of core technology infrastructure components. Funding increases were approved as part of the 2016 budget. Any surplus funds would be redirected to support departments without an available capital budget to fund their high-risk technology items.
- Establishment of a 5-year lifecycle for computers and laptops and funding of the lifecycle through existing operating accounts within ITS. Implementation was completed as part of the annual internal ITS budget review.

- Funding was identified to address the audit recommendations from the 2015 Audit of IT Risk Management and 2015 Audit of IT Security Incident Handling & Response to improve the overall information and cyber security posture within the City of Ottawa.

August 2020 management update:

- IT management has reviewed its current budget to ensure that funding is in place to mitigate prioritized risks. The operational budget for IT security and risk items was increased by approximately 80% from 2018 to 2020.
- An 'IT Renewal Fund' was created using capital dollars to fund a selection of technology projects that are considered a priority for the corporation, including projects that help IT effectively and proactively manage security risk to the organization. This fund is managed by the CIO, working with Finance Services to establish a list of projects annually, a high-level spending plan, as well as a budget plan to address the resulting operating pressures.
- The Technology Security Branch has also increased its workforce by three positions, including a dedicated resource for the security risk management function.

A new Chief Information Security / Digital Risk Officer (CISO) position has been added to the IT management team, reporting directly to the General Manager of the Innovative Client Services department. This position is responsible for ensuring that risk management is both integrated and maximized to benefit risk decision-making within the City. It is also responsible for ensuring continuous improvement of the security risk management program.

OAG assessment:

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

The Technology and Security 3 year budget comparison spreadsheet was reviewed and noted that the budget has increased from $2.315m in 2018 to $4.197m in 2020. This includes an increase in “Purchased Services” from $65,737 to over $900,000 for both 2019 and 2020. The creation of the Chief Information Security / Digital Risk Officer (CISO) role and recruitment of an experienced individual highlights the commitment to improving and targeted IT related spending, while also providing the additional security and risk expertise that was highlighted as a gap previously.

Recommendation #3

Table 4: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

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.

Original management response:

Management agrees with this recommendation.

The City Manager, in conjunction with ITS will take steps to strengthen the effective authority of CITMT as part of the work being undertaken to implement Recommendation 1. Processes will be developed to incorporate the role of a senior oversight body in the risk mitigation decision-making process. This work will be completed by Q4 2017.

2018 management update:

The Technology Security Risk Management (TSRM) governance team was created as an oversight body for risk mitigation and decision-making in Q4 2017. The TSRM has authority to provide and approve recommendations on systems that are connected to or affect the City’s overall IT environment, including any IT environments run independently by a department or board.

August 2020 management update:

See response provided for Recommendation #1.

OAG assessment:

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

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. Management provided evidence of 5 separate occasions where risks were discussed via the Teams channel. This included a number of exemptions in relation to COVID-19 and the connectivity required for remote working.

Management have stated that they find "the Teams channel to be an effective and efficient way of interacting on the mandate of the TSRM governance, especially following the forced work-from-home scenario in response to the global pandemic. This meeting medium is acknowledged in the approved Terms of Reference". Management also plans to further clarify this engagement method "as the preferred method for standard risk assessments". It is noted that one of the benefits of the Teams channel is that it addresses the previous issue of only certain individuals being aware or informed of risk approvals or exemptions.

Recommendation #4

Table 5: Status

Management update	OAG assessment
Partially complete	Complete

Audit recommendation:

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.

Original management response:

Management agrees with this recommendation.

The City Manager will take steps to strengthen and confirm the role, responsibilities and accountabilities of the Director, IT and CIO. In addition, as part of work done to implement Recommendation 1, the City Manager will consider best practices as identified in the ISACA RISK IT Framework in determining appropriate functional reporting for IT matters. This recommendation will be complete by Q4 2016.

Management update 2018:

The revised Information Security Policy (ISP) has been approved and has been updated on Ozone. Corporate communication is pending from the GM, Corporate Services and City Treasurer.

This policy confirms the role and authority of the CIO with respect to all technical and technical security risks at the City. The approved and corporately communicated IT Risk Management Framework outlines industry best practices and processes in place to effectively track and manage technical and technical security risks at the City.

The start of this project was delayed due to the corporate re-organization in late 2016. Expected completion is Q4 2018.

OAG assessment:

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

IT management has reviewed its current budget to ensure that funding is in place to mitigate prioritized risks. The operational budget for IT security and risk items was increased by approximately 80% from 2018 to 2020.

An ‘IT Renewal Fund’ was created using capital dollars to fund a selection of technology projects that are considered a priority for the corporation, including projects that help IT effectively and proactively manage security risk to the organization. This fund is managed by the CIO, working with Finance Services to establish a list of projects annually, a high-level spending plan, as well as a budget plan to address the resulting operating pressures.

The Technology Security Branch has also increased its workforce by three positions, including a dedicated resource for the security risk management function.

A new Chief Information Security / Digital Risk Officer (CISO) position has been added to the IT management team, reporting directly to the General Manager of the Innovative Client Services department. This position is responsible for ensuring that risk management is both integrated and maximized to benefit risk decision-making within the City. It is also responsible for ensuring continuous improvement of the security risk management program.

Recommendation #5

Table 6: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

That the CIO develop a robust ITRM Framework which:

- Is aligned to the ERM Framework;
- Incorporates the recommended Governance component of an ITRM framework (Refer to Recommendation #1);
- Includes clearly defined roles, responsibilities, and authorities for all City employees involved in ITRM;
- Incorporates a well-documented audit universe/inventory and a risk register;
- Incorporates a well-developed challenge mechanism conducted by trained and qualified IT professionals;
- 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.

Original management response:

Management agrees with this recommendation.

The current ERM framework will be reviewed and the ITRM framework will be enhanced to include the policies, processes and authorities for the entire corporation. Risk tolerance guidelines will be developed to include the process whereby unacceptable risks will be escalated to the appropriate authorities. The annual budgeting exercise will include a risk mitigation component where unfunded risk reduction costs will be identified. This recommendation will be complete by Q4 2017.

2018 Management update:

The IT Risk Management (ITRM) framework has been approved and communicated corporately. This document outlines the executive roles and governance of technical and technical security risks at the City. This includes a formal risk exemption process and an established Technical Security Risk Management (TSRM) governance team, as well as an annual risk validation process, where priorities will be set based on risks that exceed established thresholds.

The ITRM Framework has been developed in alignment with the current ERM framework. An operational risk register is in place, which includes tracking and management of technical and technical security risk and mitigation action follow-ups for completion. Risk Register dashboard displays are produced on a department level, service area, and an enterprise view.

The annual risk validation process is in progress and will be completed by Q4 2018.

OAG assessment:

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

The assessment is also in relation to Recommendation #3.

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. Management provided evidence of 5 separate occasions where risks were discussed via the Teams channel. This included a number of exemptions in relation to COVID-19 and the connectivity required for remote working.

Management have stated that they find "the Teams channel to be an effective and efficient way of interacting on the mandate of the TSRM governance, especially following the forced work-from-home scenario in response to the global pandemic. This meeting medium is acknowledged in the approved Terms of Reference". Management also plans to further clarify this engagement method "as the preferred method for standard risk assessments".

It is noted that one of the benefits of the Teams channel is that it addresses the previous issue of only certain individuals being aware or informed of risk approvals or exemptions. Given the COVID-19 situation and remote working, we recognize the benefits of using this medium, as long as the content is able to be archived and retained for future reference.

Additionally, Management should consider if there would be benefit in more formal documentation of the risk assessment meetings themselves, to capture the risk decisions made, and so the information is retained for future reference.

Recommendation #6

Table 7: Status

Management update	OAG assessment
Partially complete	Complete

Audit recommendation:

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;
- Specifies the skill sets and training required of those responsible for completion of departmental components of the ITRM documents;
- Embeds the strengthened role of the CIO.

Original management response:

Management agrees with this recommendation.

Policies and procedures will be developed to incorporate the ITRM framework with appropriate challenge mechanisms. Requisite skills and training will be identified and included as part of the phasing in of the framework. This recommendation will be complete by Q4 2017.

2018 management update:

The revised and approved ISP confirms the role and authority of the CIO with respect to all technical and technical security risks at the City.

The annual risk validation process (part of the risk framework) is currently being documented and it is dependent on risk assessment processes being done by qualified technical resources for all technical change. IT is working with the Business Support Service units for finalization of the annual risk validation processes.

There was a delay in the project start due to the 2016 corporate re-organization. Expected completion is Q4 2018.

2020 management update:

See response provided for Recommendation #1.

OAG assessment:

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

We noted that a documented IT Risk Management Framework (ITRM) v2.0 outlines the overall governance model related to risk management and is in alignment with the City's ERM framework.

The Annual Risk Validation (ARV) process is now in place and the 2019 "Annual Risk Validation Report" was reviewed, dated January 24, 2020. It is stated that "the ARV process establishes a citywide means to validate assessed technology and technology security risks that are tracked by Information Technology Services with a risk score of High". The results of the ARV process validated 23 risks and added 1 risk in relation to Transportation Services.

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. Management provided evidence of 5 separate occasions where risks were discussed via the Teams channel. This included a number of exemptions in relation to COVID-19 and the connectivity required for remote working. Management stated that they prefer to keep the meetings informal and there are no documented minutes to the meetings.

Additionally, Management stated that they find "the Teams channel to be an effective and efficient way of interacting on the mandate of the TSRM governance, especially following the forced work-from-home scenario in response to the global pandemic. This meeting medium is acknowledged in the approved Terms of Reference". Management also plans to further clarify this engagement method "as the preferred method for standard risk assessments". It is noted that one of the benefits of the Teams channel is that it addresses the previous issue of only certain individuals being aware or informed of risk approvals or exemptions.

Recommendation #7

Table 8: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

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;
- Develop departmental processes which ensure that all components of the business line are included in required ITRM documents;
- 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.

Original management response:

Management agrees with this recommendation.

City management, with assistance from ITS, will include training, document preparation, risk escalation, challenge processes, tracking mechanisms and reporting as part of the enterprise wide roll-out of the ITRM framework. This recommendation will be complete by Q4 2017.

2018 management update:

The IT Risk Management (ITRM) framework has been approved and communicated corporately.

Supporting processes outline the methodologies, templates and tools as well as the roles and responsibilities to complete risk assessments and track those risks and mitigations for all technology changes. This includes a formal risk exemption process and an established Technical Security Risk Management (TSRM) governance team, as well as an annual risk validation process, where priorities will be set based on risks that exceed established thresholds.

The annual risk validation process is currently being documented with the involvement of the Business Support Service units.

2020 management update:

See response provided for Recommendation #1.

In addition, IT relies on the following for identification of technology and technology security risks:

1. Security standards awareness for IT support staff to flag risks,
2. Vulnerability scanning practices,
3. All Threat and Risk Assessments (TRA) are now tracked in our Risk Register for any mitigation/exemption follow-ups,
4. Infrastructure life-cycling based on vendor support documents and corporate requirements, and
5. Application life-cycling based on the TIME (Tolerate, Invest, Migrate, Eliminate) model is tracked in the IT Configuration Management Database (CMDB).

OAG assessment:

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

As evidence of additional Threat Risk Assessments (TRA) being conducted as part of changes to existing services, a TRA report for Radio Logger equipment (V2.0 dated 12 August 2020) was reviewed. The TRA was conducted due to the technology undergoing an upgrade ("migrating from Exacom G2 to Exacom G3 radio loggers – the latest version"). The Report summarizes the results of the security assessment of the Exacom migration, and the resulting radio logging infrastructure.

The City has produced an updated IT Risk Management Framework document v2.0 on December 13, 2019. The updated document is now more aligned to the Enterprise Risk Management Policy (ERMP) and contains Roles and Responsibilities for the Technology Security Risk Management Team (TSRM); CIO; Department Leadership Team; Technology Security Branch (TSB) and Business Support Services.

Additional evidence was provided in relation to the “Security Team Experience 2020” tracking spreadsheet. This captures the certifications and training (including conference attendance) for those in the Security team who may perform risk assessments. It was noted that there was extensive security training and certifications for those in key positions related to making security risk decisions.

As noted under previous findings, a TSRM channel in Microsoft Teams has been created for members of the TSRM governance body and is now used for collaboration on risk discussions and to capture and record approvals. Management provided evidence of 5 separate occasions where risks were discussed via the Teams channel. This included a number of exemptions which were approved in relation to COVID-19 and the connectivity required for remote working.

Recommendation #8

Table 9: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

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.

Original management response:

Management agrees with this recommendation.

The principle of continuous improvement will be applied as the ITRM framework program is phased in to ensure continuous and improved identification and assessment of IT risk and related mitigation strategies. A senior oversight body, currently being established, will oversee the maturation of the ITRM framework. Once the ITRM framework is implemented, ITS will conduct assessments of new or emerging IT mitigation strategies on an annual basis.

2018 management update:

Continuous improvement principles are applied to the IT Risk Management Framework and supporting processes. In addition, the framework and processes are to be reviewed on an annual basis as a part of the annual risk validation process. The Technical Security's branch objectives and key results (OKR) include annual reviews of tools and methodologies to ensure they are current to industry best practices.

The annual risk validation process is currently being documented with the involvement of the Business Support Service units.

This project was delayed due to the 2016 corporate re-organization. Expected completion is Q4 2018.

August 2020 management update:

A Continuous Improvement Section is documented in the Annual Risk Validation Process for governance review by the Technical Security Risk Management team. As part of the continuous improvement of the overall risk management process, the following documents are reviewed annually:

- ITRM Framework
- IT Risk Assessment Process
- IT Risk Register Process Manual
- Exemption Process

OAG assessment:

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

The OAG has performed a review of the latest version 2.0 the IT Risk Management Framework (ITRM) document that is dated on December 13, 2019. We noted the revision section includes updates to TSRM roles and responsibilities; approval levels and sample 5x5 Risk Mapping; and clarification on the Annual IT Risk Validation.

The Annual Risk Validation (ARV) process is now in place and the 2019 “Annual Risk Validation Report” was reviewed, dated January 24, 2020. It is stated that “the ARV process establishes a citywide means to validate assessed technology and technology security risks that are tracked by Information Technology Services with a risk score of High”. The results of the ARV process validated 23 risks and added 1 risk in relation to Transportation Services. It notes that all risk assessments and validation work were conducted by trained Technology Security team members.

Table 10: 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.