Office of the Auditor General

Follow-up to the 2015 Audit of IT Risk Management

Tabled at Audit Committee
May 29, 2019

Table of Contents

Executive summary

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

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

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

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

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

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

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

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

   Specific findings from the original audit included:

   - Lack of an Information Technology Risk Management (ITRM) Framework including a comprehensive Governance component and clear and consistent responsibilities and accountabilities for City executives and management;
   - The decentralized method of prioritizing, selecting and funding IT initiatives may result in approved projects that are not aligned with corporate priorities, and significant risk was identified that high priority IT risks are not being adequately addressed on a timely basis where funding is not readily available to the business owner;
   - The Corporate Information Technology Management Team (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 to the CIO and lines of authority are not always clear, and the CIO's authorities and responsibilities for City-wide IT risks are not formally defined.

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

   Specific findings from the original audit included:

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

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

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

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

Specific findings from the original audit included:

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

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

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

Table 1: Summary of status of completion of recommendations

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

The recommendations found to be partially completed included:

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

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

- *Clearly establishes the basis for a corporate risk culture, including risk tolerance and risk appetite guidelines.* The City has made improvements by establishing its risk appetite and tolerance guidelines, including the collection of 53 service area risks, the introduction of a formalized risk exemption process, and an annual risk validation process is under development.
- Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are considered for inclusion in the Annual Corporate IT Plan based on risk/priority, regardless of whether there is pre-approved funding identified. We have noted that the ITS plan is focused on capital expenditure as well as the development and/or update of key processes, and funding is linked with Objectives and Key Results. However, the City of Ottawa's funding models have not facilitated the mitigation of operational IT risks related to the 2015 Audit of IT Security Incident Handling & Response finding [redacted], indicating funding for operational IT risks may not have kept pace.

- *That the City Manager and City Treasurer undertake an assessment of IT spending to explore alternative funding models which will provide better alignment between mitigation of prioritized City-wide IT risks and funds available/provided and provide long term savings through improved, targeted IT spending.* The City has established new funding models to allow the funding for unacceptable IT risks. However, the City of Ottawa's funding models have not facilitated the mitigation of operational IT risks related to the 2015 Audit of IT Security Incident Handling & Response finding [redacted], indicating funding for operational IT risks may not have kept pace.
- *That the City Manager take steps to strengthen the effective authority of CITMT including expanding reviews to include all City-wide IT risks and proposed/recommended mitigation strategies.* The City has established the Technology Security Risk Management Team as an oversight body for risk mitigation and decision making. We noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions / exceptions from standard procedures which affects governance and oversight of IT risks.

- *That the City Manager take steps to strengthen and confirm the role, responsibility and accountability of the Director, ITS and CIO position including consideration of alignment with the best practices identified in the ISACA RISK-IT Framework as well as functional reporting of all City departments and agencies to the CIO for all IT matters.* The City has updated its Information Security Policy and prepared an Information Technology Risk Framework outlining the roles and responsibilities of key positions with respect to its IT risks. We noted that these practices are aligned with the ISACA RISK-IT Framework, and require the completion of the annual risk validation process currently under development as a key part of tracking and managing IT risks.

- *That the CIO develop a robust ITRM Framework which:*

  - *Is aligned to the ERM Framework.* We noted that an ITRM Framework has been developed and that alignment is in place.
  - *Incorporates the recommended Governance component of an ITRM framework (Refer to Recommendation #1).* As above, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions or exceptions from standard procedures, which affects governance and oversight of IT risks.
  - *Includes clearly defined roles, responsibilities, and authorities for all City employees involved in ITRM.* As above, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions or exceptions from standard procedures (which affects governance and oversight of IT risks).

- *Incorporates a well-documented audit universe/inventory and a risk register.* An IT inventory universe has not been completed that would serve to support identification of potential IT risks. A risk register exists and a recent quarterly review was performed.
- *Incorporates a well-developed challenge mechanism conducted by trained and qualified IT professionals.* At the time of the assessment, we observed two mechanisms that are involved in the IT risks challenge function: the exemption/exception process which was observed to have inconsistent approval requirements in City practices, and the annual risk validation process which was in development and we noted that resources assigned to this process required additional support in terms of training, experience and time available to the establishment of this process.
- *Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are communicated to Senior Management in a comprehensive and effective manner.* An operational risk register is in place, which is used to communicate risks using a dashboard. Business Support Services personnel are assigned as the departmental contact of all risk management activities, and were noted to lack technology understanding and/or formal risk training to assist them with identifying potential IT risks and participating in IT risk assessment.

- *That the CIO, in conjunction with the development of the ITRM Framework, develop a supporting policy and procedure suite that:*

  - *Incorporates all required processes for completion of the ITRM Framework including a robust challenge mechanism.* As above, we noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework, and we noted that the exemption/exception process was observed to have inconsistent approval requirements.
  - *Specifies the skill sets and training required of those responsible for completion of departmental components of the ITRM documents.* We did not observe evidence that skill sets and training specifications for departmental components of the ITRM documents were specified.

- *Embeds the strengthened role of the CIO.* We noted that significant progress was made to further define the CIO role since the previous audit. However, the role of the CIO in the City's current IT risk policies and processes is inconsistent regarding approval requirements for exemptions or exceptions from standard procedures.

- *That all City departments, with direction and support from ITS:*
  - *Ensure departmental staff preparing ITRM documents have the requisite skills and tools to adequately and completely prepare all required ITRM documents.* As above, Business Support Services personnel are assigned as the departmental contact of all risk management activities, and were noted to lack technology understanding and/or formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessment. Additionally, we noted that the approach to perform a quick review process to capture existing IT risks using existing TRA information may not properly identify all IT risks at the City requiring assessment, and additional ITS resources to perform risk assessment and related mitigation planning and monitoring activities may be required.
  - *Develop departmental processes, which ensure that all components of the business line are included in required ITRM documents.* We noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework.
  - *Develop review and challenge mechanisms designed to ensure that all ITRM documents are completed to an appropriate level of granularity which fully facilitates the understanding of IT risks, impact and the management and tracking of strategies related to the mitigation of IT risks.* As above, we noted the annual risk validation process was in development at the time of the assessment, which is a key part of the ITRM Framework, and we noted that the exemption/exception process was observed to have inconsistent approval requirements.

The recommendations that were unable to be assessed included:

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

Conclusion

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

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

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

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

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

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

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

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

Acknowledgement

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

Detailed report – Assessment of implementation status

To complete the assessment, the auditors reviewed key City policy and process documents, including the ITRM Framework 1.0, risk exemption process, TRA-Risk Assessment process, Information Security Policy, etc.

The auditors also conducted numerous interviews with various ITS information security team members including the City CIO, Manager of Technology Solutions, Manager of Technology Security as well as various IT security analysts.

The audit also required the review of the risk assessment exception process. As part of the review, the auditors selected the complete list of exceptions since the process was put in place, including:

- Cisco Jabber – June 2018;
- SAP Hana – September 2018;
- OPH Split Tunnel – February 2018;
- O365 Password Reset – January 2018;
- Microsoft Teams – March 2018;
- EPS Screen Saver – September 2017; and
- Elections Server Patching – August 2018.

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
Partially complete	Partially 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.

Management update:

The Information Security Policy (ISP) has been approved and is posted on Ozone. The IT Risk Management (ITRM) framework has been approved and communicated corporately. These documents outline 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 ISP corporate communication is currently being finalized and development of the annual risk validation process is in progress; these will be completed by Q4 2018.

OAG assessment:

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

We have noted that the City has released a documented IT Risk Management Framework on January 18, 2018. This newly developed IT Risk Management Framework defines Risk Governance into four core activities:

- Engaging City departments on IT risks that they own;
- Reviewing IT risks, at the appropriate level, as described in the ITRM Workflow;
- Approving action plans to mitigate risks above identified thresholds; and
- Updating City policies and standards for ITRM.

We have noted that the newly developed framework aligns with the City's existing Enterprise Risk Management (ERM) framework.

The framework also identifies the executive roles and governance of technical and technical security risks at the City. This includes:

- Senior leadership team who is accountable for the overall ITRM program;
- Departmental leadership team who are accountable for the management of IT and information security risks within their own department;
- Technology Security Risk Management Team who provides the operational governance for the ITRM program including escalations and approval of exceptions;
- Chief Information Officer who is responsible to the TSRM team in managing the ITRM program, and accountable for ITRM of all shared IT infrastructure managed by ITS;
- Technology Security Branch (TSB) who is functionally responsible for many components of the ITRM program; and
- Business Support Services (BSS) who are the departmental point of contact for all risk management activities.

Furthermore, we have noted that the Technology Security Risk Management (TSRM) Team are made up of:

- General Manager of Corporate Services Department (CSD);
- City Clerk and Solicitor; and
- Chief Information Officer.

It is important to note that although the TSRM team members understand potential risk as it applies to their department, they may not have the skillset and/or experience in information technology to fully comprehend the risk to the City. As such, it is the CIO's responsibility to ensure that the TSRM fully understands the technology risk and to engage subject matter experts (SMEs) as needed.

The TSRM are responsible for the following:

- Ongoing program management based on the IT Risk Register, Dashboard and annual IT Risk Assessment;
- Escalations from the CIO and program-wide changes or approvals;
- Escalation and reporting on risks to Senior Leadership Team (SLT);
- Recommending risk treatment and exceptions to SLT; and
- IT Risk Management Policy and standards review and approval.

We additionally noted that Business Support Services (BSS) are specifically responsible for the following tasks as they relate to the City's risk management program:

- Act as a liaison between TSB and their department in areas of ITRM;
- Communicate potential IT risks to TSB for inclusion in the citywide IT Risk register;
- Participate in and support the challenge function and the conduct of the annual enterprise IT Risk assessment;
- Communicate the IT risk outcomes from departmental risk management activities; and
- CSD BSS will also act as a liaison between departmental BSS units in support of IT risk assessment and consolidation process.

BSS are now responsible for identifying and communicating potential IT risks and participating in risk assessments and in many cases are referred to by staff as "risk practitioners"; however, BSS resources lack technology understanding and formal risk training to assist them with these responsibilities.

As a result of the above, roles and responsibilities have become more clearly defined with the introduction of the ITRM Framework. The City has made further improvements by establishing its risk appetite and tolerance guidelines, including the collection of 53 service area risks, and the introduction of a formalized risk exemption process.

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 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 neither the SLT nor the TSRM approved the seven exemptions reviewed. For example, for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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.

We have also noted that the City has begun the development of an annual technology risk validation process. At the time of our audit, this process was still under development. Given the scope and complexity of the risk management initiatives, the City should consider whether resource requirements should be further allocated to perform IT risk management functions.

Impact:

A lack of appropriate governance of the City's IT risks 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 #2

Table 3: Status

Management update	OAG assessment
Complete	Partially 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.

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.

OAG assessment:

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

We have noted that ITS have developed a three-year strategic plan in 2017[2]. This plan has as a goal to provide the following by 2020:

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

To meet these objectives, we have noted that ITS have documented a number of initiatives that will be completed, these include:

- Create and maintain a ‘Best in Class’ security environment for the corporation;
- Ensure all informational technology assets are protected appropriately in an ever-changing security landscape;
- Right-size the use of High Availability (HA) technologies to meet the organization’s needs;
- Mature IT Service Management (e.g. change control, service delivery) practices to optimize the investment of resources;
- Enhance and modernize application infrastructure; and
- Enable new and advanced SAP features.

[2] ITS Strategic Plan 2018-2020.pdf

As per the updated IT spending initiatives, the CIO has established a new ITS project intake process. IT Business Analysts work with client groups to determine if a project is small or large using a brief list of simple scoping questions. Small projects will proceed into the project life cycle for implementation once resources are assembled. Large projects will require a high-level review and resource discussion with a subset of Senior Leaders before completing a detailed business case. IT Services will coordinate the completion of a detailed Business Case with input from all relevant departments, including the detailed business requirements provided by the client. The Steering Committee is responsible for reviewing the Business Case and managing the direction of the project.

We have noted that the ITS plan is focused on capital expenditure as well as the development and/or update of key processes, and funding is linked with Objectives and Key Results. However, the City of Ottawa's funding models have not facilitated the mitigation of operational IT risks related to the 2015 Audit of IT Security Incident Handling & Response finding [redacted], indicating funding for operational IT risks may not have kept pace.

During interviews with ITS, the OAG was advised that ITS has not significantly adjusted the City's operational budget from year to year to accommodate emphasis on its workforce, and hiring of new ITS staff has stayed static for a number of years. Additionally, numerous members of the ITS team have noted that the organization lacks experienced staff to complete many of the projects outlined in the City's strategic ITS plan.

Impact:

Mitigation of prioritized City-wide IT risks requires both capital and operating funding, and having sufficient and experienced human resources is crucial to effectively mitigate IT risks.

Recommendation #3

Table 4: Status

Management update	OAG assessment
Complete	Partially 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.

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.

OAG assessment:

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

We have noted that the City has implemented the Technology Security Risk Management team (TSRM). The TSRM are responsible for the following:

- Ongoing program management based on the IT Risk Register, Dashboard and annual IT Risk Assessment;
- Escalations from the CIO and program-wide changes or approvals;
- Escalation and reporting on risks to SLT;
- Recommending risk treatment and exceptions to SLT; and

- IT Risk Management Policy and standards review and approval.

As described under Recommendations 1, 3, 4, 5, 6 and 7, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions / exceptions from standard procedures (which affects governance and oversight of IT risks).

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 neither the SLT nor the TSRM approved the seven exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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 of the City's IT risks 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 #4

Table 5: Status

Management update	OAG assessment
Partially complete	Partially 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:

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:

We have reviewed the revised Information Security Policy (ISP) last revised on July 16, 2018. The ISP details the roles and responsibilities as they relate to IT services for the City. This includes a description for the following roles:

- City Manager;
- Chief Information Officer (CIO);
- Department heads;
- Manager, Technology Security;
- Systems administrators; and
- Employees.

We have noted that the City has released a documented IT Risk Management Framework on January 18, 2018. This newly developed IT Risk Management Framework divides Risk Governance into four core activities:

- Engaging City departments on IT risks that they own;
- Reviewing IT risks, at the appropriate level, as described in the ITRM Workflow;
- Approving action plans to mitigate risks above identified thresholds; and
- Updating City policies and standards for ITRM.

We reviewed the ISACA Risk IT Framework[3], last published in 2009 and noted that the City's IT Risk Management Framework has been developed in line with ISACA's framework, which states that organizations shall:

- Establish and maintain a common risk view including performing regular IT risk assessments;
- Propose IT risk tolerance thresholds;
- Approve IT risk tolerance;
- Align IT risk policy;
- Promote IT risk-aware culture; and
- Encourage effective communication of IT risk.

[3] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

We noted that the City's framework aligns to the ISACA Risk IT Framework. We noted that as part of the City's framework, ITS are involved in the task of reviewing IT risks, at the appropriate level, as described in the ITRM Workflow. As part of this requirement, the City has begun the development of an annual risk validation process. The development of the process has yet to be completed. The validation process involves reviewing the findings from past threat risk assessments and adding these to the ITS risk register. Once risks are added, a threat risk assessment (TRA) is required. ITS are hoping to have members of the IT security team perform the review. ITS have noted that there are approximately 120 risk items in the register (with the exception of the six service areas that have not been reviewed yet). It was noted during discussions with ITS that IT security currently has four full time employees and one contractor to conduct TRAs. Given the number of TRAs to be completed and the number of resources available, it will be difficult to perform timely assessments of all risks, taking into account that new risks are being added daily.

We were advised by staff that ITS lacked sufficient experienced and capable staff to conduct the TRAs. This was highlighted when it was noted that initially, as part of the reconciliation of the risks from the various 53 service areas, ITS had planned to perform a pilot on a number of service areas to determine the effort required to capture IT risks. Following the pilot of 1-2 service areas, it was decided by management that proceeding to capture IT risks by service area through risk information sessions was deemed not to be worth the level of effort. Instead, an approach with a quick review process using existing TRA information was performed to produce service area risk profiles. The OAG notes that this approach, coupled with an incomplete IT universe, may not successfully identify all existing IT risks at the City.

As described under Recommendations 1, 3, 4, 5, 6 and 7, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions / exceptions from standard procedures (which affects governance and oversight of IT risks, as well as the role, responsibility and accountability of the Director, ITS and CIO position).

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 neither the SLT nor the TSRM approved the seven exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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 of the City's IT risks 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 improper, 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 #5

Table 6: Status

Management update	OAG assessment
Partially complete	Partially 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.

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 partially complete.

We have noted that the City have released a documented IT Risk Management Framework on January 18, 2018. This newly developed IT Risk Management Framework defines Risk Governance into four core activities:

- Engaging City departments on IT risks that they own;
- Reviewing IT risks, at the appropriate level, as described in the ITRM Workflow;
- Approving action plans to mitigate risks above identified thresholds; and
- Updating City policies and standards for ITRM.

The framework also identifies the executive roles and governance of technical and technical security risks at the City. This includes:

- Senior leadership team who is accountable for the overall ITRM program;
- Departmental leadership team who are accountable for the management of IT and information security risks within their own department;
- Technology Security Risk Management Team who provides the operational governance for the ITRM program including escalations and approval of exceptions;

- Chief Information Officer who is responsible to the TSRM team in managing the ITRM program, and accountable for ITRM of all shared IT infrastructure managed by ITS;
- Technology Security Branch (TSB) who is functionally responsible for many components of the ITRM program; and
- Business Support Services who are the departmental point of contact for all risk management activities.

We noted that the newly developed framework aligns with the City's existing Enterprise Risk Management (ERM) framework. A full inventory of the IT universe across the City (applications, business owners, networks, interdependencies, etc.) has not been defined, which would aid as a starting point to understand and identify IT risks. An operational risk register is in place, which is used to communicate risks using a dashboard. We observed that a recent quarterly review was performed "Technology Security Risk Register Quarterly Overview", October 2018.

We noted that Business Support Services (BSS) are specifically responsible for the following tasks as they relate to the City's risk management program:

- Act as a liaison between TSB and their department in areas of ITRM;
- Communicate potential IT risks to TSB for inclusion in the citywide IT Risk register;
- Participate in and support the challenge function and the conduct of the annual enterprise IT Risk assessment;
- Communicate the IT risk outcomes from departmental risk management activities; and
- CSD BSS will also act as a liaison between departmental BSS units in support of IT risk assessment and consolidation process.

BSS are now responsible for identifying and communicating potential IT risks and participating in risk assessments and in many cases are referred to by staff as "risk practitioners"; however, BSS resources lack technology understanding and formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessment.

Furthermore, we have noted that the Technology Security Risk Management (TSRM) Team are made up of:

- General Manager of Corporate Services Department (CSD);
- City Clerk and Solicitor; and
- Chief Information Officer.

The TSRM are responsible for the following:

- Ongoing program management based on the IT Risk Register, Dashboard and annual IT Risk Assessment;
- Escalations from the CIO and program-wide changes or approvals;
- Escalation and reporting on risks to SLT;
- Recommending risk treatment and exceptions to SLT; and
- IT Risk Management Policy and standards review and approval.

As described under Recommendations 1, 3, 4, 5, 6 and 7, we noted that the City's current IT risk policies and processes are inconsistent regarding approval requirements for exemptions / exceptions from standard procedures (which affects governance and oversight of IT risks, as well as the role, responsibility and accountability of the Director, ITS and CIO position).

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 neither the SLT nor the TSRM approved the seven exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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 of the City's IT risks 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 could 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 #6

Table 7: Status

Management update	OAG assessment
Partially complete	Partially 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.

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.

OAG assessment:

We have noted that the City has begun the development of an annual technology risk validation process. At the time of our audit, this process was still under development. Given the scope and complexity of the risk management initiatives, the City should consider whether resource requirements should be further allocated to perform IT risk management functions.

We have noted that Business Support Services (BSS) are specifically responsible for the following tasks as they relate to the City's risk management program:

- Act as a liaison between TSB and their department in areas of ITRM;
- Communicate potential IT risks to TSB for inclusion in the citywide IT Risk register;
- Participate in and support the challenge function and the conduct of the annual enterprise IT Risk assessment;
- Communicate the IT risk outcomes from departmental risk management activities; and
- CSD BSS will also act as a liaison between departmental BSS units in support of IT risk assessment and consolidation process.

BSS are now responsible for identifying and communicating potential IT risks and participating in risk assessments and in many cases are referred to by staff as "risk practitioners"; however, BSS resources lack technology understanding and formal IT risk training to assist them with identifying potential IT risks and participating in IT risk assessment.

As identified in Recommendations 1, 3, 4, 5, 6 and 7, 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, and impacts the defined role and responsibilities of the CIO).

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 neither the SLT nor the TSRM approved the seven exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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.

Additionally, we did not observe evidence that skill sets and training specifications for departmental components of the ITRM documents were specified.

Impact:

A lack of appropriate governance of the City's IT risks 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 could result in erroneous or delayed identification of critical IT risks to the City, leading to risk-taking without a full understanding of the potential nature or severity of consequences.

Recommendation #7

Table 8: Status

Management update	OAG assessment
Complete	Partially 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.

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.

OAG assessment:

We have reviewed the Information Security Policy (ISP) last revised on July 16, 2018. The ISP details the roles and responsibilities as they relate to IT services for the City. This includes a description for the following roles:

- City Manager;
- Chief Information Officer (CIO);
- Department heads;
- Manager, Technology Security;
- Systems administrators; and
- Employees.

We have noted that the City have released a documented IT Risk Management Framework on January 18, 2018. This newly developed IT Risk Management Framework defines Risk Governance into four core activities:

- Engaging City departments on IT risks that they own;
- Reviewing IT risks, at the appropriate level, as described in the ITRM Workflow;
- Approving action plans to mitigate risks above identified thresholds; and
- Updating City policies and standards for ITRM.

We reviewed the ISACA Risk IT Framework[4], last published in 2009 and noted that the City's IT Risk Management Framework has been developed in line with ISACA's framework, which states that organizations shall:

- Establish and maintain a common risk view including performing regular IT risk assessments;
- Propose IT risk tolerance thresholds;
- Approve IT risk tolerance;
- Align IT risk policy;
- Promote IT risk-aware culture; and
- Encourage effective communication of IT risk.

[4] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

We noted that the City's framework aligns to the ISACA Risk IT Framework. We noted that as part of the City's framework, ITS are involved in the task of reviewing IT risks, at the appropriate level, as described in the ITRM Workflow.

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

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

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

Given the scope and complexity of the risk management initiatives, the City should consider whether resource requirements should be further allocated to perform IT risk management functions.

As identified in Recommendations 1, 3, 4, 5, 6 and 7, 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, and impacts the defined role and responsibilities of the CIO).

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 neither the SLT nor the TSRM approved the seven exemptions reviewed (for example for an Election Server Patching exemption and an exception related to the storage of personal email addresses and phone numbers in the US as part of a cloud deployment) were not approved by the SLT or TSRM, they were approved by either the CIO and/or the Manager of IT Security. As a result, we are unable to assess whether these exceptions / exemptions followed the appropriate policy/process; though both the ITRM and the Technical Security Risk Exemption Process suggest that additional approvals may have been necessary from either the SLT or the TSRM. 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 of the City's IT risks 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 improper, 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 #8

Table 9: Status

Management update	OAG assessment
Complete	Unable to assess

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.

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.

OAG assessment:

The OAG has performed a review of version 1.0 the IT Risk Management Framework (ITRM) document that was released on January 28, 2018. We noted the revision section only indicates the approval of the document on January 17, 2018. Given the strategy is only reviewed once per year, the OAG were not able to identify any changes and/or improvements to the ITRM framework.

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.