



City Auditor's Office

# Integrated Risk Management Audit

May 12, 2021

**THIS PAGE LEFT INTENTIONALLY BLANK**

## Table of Contents

<b>Executive Summary</b> .....	<b>5</b>
<b>1.0 Background</b> .....	<b>7</b>
<b>2.0 Audit Objective, Scope and Approach</b> .....	<b>8</b>
2.1 Audit Objective .....	8
2.2 Audit Scope .....	8
2.3 Audit Approach .....	8
<b>3.0 Results</b> .....	<b>9</b>
3.1 Continuous Improvement .....	10
3.2 Full Accountability for Risks .....	11
3.3 Application of Risk Management in all Decisions .....	13
3.4 Continual Communications .....	14
3.5 Integration.....	14
3.6 Risk Appetite and Tolerance .....	15
<b>4.0 Observations and Recommendations</b> .....	<b>16</b>
4.1 IRM Framework Performance Assessment.....	16
4.2 IRM Risk Appetite and Tolerance.....	17
4.3 Performance Measures.....	19
4.4 Service Risk Register Assessment Process.....	20
4.5 Service Risk Register Process .....	22
<b>Appendix</b> .....	<b>24</b>
<b>Maturity Continuum Assessment</b> .....	<b>24</b>

The City Auditor's Office conducted this audit in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

## Executive Summary

Council adopted the Integrated Risk Management (IRM) Policy (CC011), which was last amended in 2020, to embed a more proactive, corporate-wide and systematic approach to managing risks that impact The City of Calgary's (The City's) ability to achieve its results. The City developed a structured IRM Framework<sup>1</sup> and supporting processes to guide risk management. Where risks are not identified, assessed, and managed, The City is at risk of incurring unnecessary costs and service disruption.

The City Auditor's Office conforms to The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing (Standards). Under the Standards, the City Auditor's Office is required to periodically audit the effectiveness and contribute to the improvement of risk management processes of the organization. As a result, this recurring operational audit assessing the effectiveness of the IRM Framework was included on the City Auditor's Office 2019-2020 Audit Plan.

The objective of this audit was to assess the effectiveness of the IRM Framework by independently validating the IRM Team's 2020 self-assessment against the 2011 Canadian Standards Association Risk Management Maturity Continuum and Assessment Criteria and associated attributes<sup>2</sup>:

- Continual Improvement;
- Full Accountability for Risks;
- The Application of Risk Management in all Decision Making;
- Continual Communications; and
- Full Integration into the Organization's Governance Structure.

We validated the IRM Team's 2020 self-assessment and determined, that overall, the IRM Framework is at an enhanced level of maturity. The IRM Team has made significant progress in advancing the maturity of the IRM Framework, since we last completed an audit in 2014. They have moved past basic risk management practices and are focused on continually maturing and improving risk management practices. We raised five recommendations that are intended to help achieve clarity on the future strategic direction and maturity of the IRM Framework, and identify areas where the IRM Team can build on and improve current processes that support continuous improvement of the IRM Framework.

Specifically, we recommended the IRM Team make a collective decision with the Executive Leadership Team on the desired level of maturity which will include further engagement with Audit Committee. This will help focus continuous improvement efforts and support the effective utilization of resources. There should also be a formal process to periodically evaluate Framework performance that includes input and direction from all relevant stakeholders. In addition, the IRM Team should expand on current Risk Appetite and Tolerance Guidelines to include approved levels for both strategic and operational risk to support effective decision making within The City.

---

<sup>1</sup> The City's framework is based on International Organization for Standardization guidance for risk management ISO 31000:2018.

<sup>2</sup> Canadian Standards Association Risk Management Maturity Continuum and Assessment Criteria as defined in the Implementation Guide to CAN/CSA-ISO 31000, Risk Management Principles and Guidelines (Q31001-11, March 2011).

We reviewed the Principal Corporate Risk Process and the Service Risk Register Process and noted they are both well established and defined bi-annual processes that support accountability for risk management. We also reviewed specific continual improvement activities including the Service Risk Register assessment process, the annual risk maturity survey, and how feedback from the e-learning course and other continuous improvement mechanisms flows into IRM Program work-plans. These processes are working well, however we recommended enhancements to the qualitative assessment process to support consistent identification of services in need of assistance, and improvements in Service Risk Register quality and value from year to year.

We also reviewed the IRM Program's seven performance measures. Although performance measures are generally aligned to program goals, we recommended the IRM Team re-evaluate the measures to ensure they are relevant and measurable. Measures should be periodically re-evaluated to effectively gauge progress towards IRM Program goals.

The IRM Team agreed to all recommendations and has committed to set action plan implementation dates no later than December 31, 2022. The City Auditor's Office will follow-up on all commitments as part of our ongoing recommendation follow-up process.

## 1.0 Background

The City Auditor's Office conforms to The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing (Standards). Under the Standards, the City Auditor's Office is required to periodically audit the effectiveness and contribute to the improvement of risk management processes of the organization. An effective integrated risk management (IRM) Framework enhances The City of Calgary's (The City's) ability to achieve desired results including delivery of services to citizens by establishing a reliable basis for decision making and planning. Where risks are not identified, assessed, and managed, The City is at risk of incurring unnecessary costs and service disruption. As a result, this recurring operational audit assessing the effectiveness of the IRM Framework, was included on the City Auditor's Office 2019-2020 Audit Plan.

The City Auditor's Office completed the last IRM audit in 2014 (Integrated Risk Management Audit-AC2014-0295). The audit independently validated the maturity self-assessment conducted by the City Manager's Office and assessed how effectively the IRM Framework was meeting the needs of the organization. We concluded in that audit that IRM practices generally met the principles of The City's IRM Policy (CC011) and our results supported the City Manager's Office's self-assessment of a "low enhanced" level of maturity, that is, a combination of maturing and basic risk management practices.

On February 3, 2020, the IRM Policy was amended to reflect the opportunity to capitalize on risk and create a culture that embraces the appropriate levels of risk. In addition, amendments aligned with the ISO 31000:2018 International Standard, which is the foundation of The City's IRM Framework. The purpose of the policy is to embed a more proactive, corporate-wide and systematic approach to managing risks that impact The City's ability to achieve its results. Under the amended IRM Policy, the City Manager continued to be responsible for risk management throughout The City.

The City's IRM Framework guides risk management practices to inform decision making and consists of a structured framework and supporting processes categorized in four pillars:

1. Governance and Oversight
2. Integration with Strategic Direction
3. Established Practices and Processes
4. Review and Continuous Improvement

Corporate Initiatives, a division of the Chief Financial Officer's Department, is responsible for leading the corporate IRM Program, which supports the IRM Framework and contributes to The City's risk maturity. Although the IRM Program supports the advancement of risk management across the organization, it is the collective responsibility of all employees to manage risks within their respective areas. There are three staff dedicated to the IRM Program, who will be referred to as the IRM Team throughout this report.

The IRM Program's three goals to advance the IRM Framework in 2020 were to: develop a robust risk culture, mature The City's IRM Program and improve risk communication and coordination. The IRM Team reported to ELT (ALT2020-0577 –Attachment 4) the focus of the Program in 2020 was to continuously evolve and advance a risk aware culture, encouraging every employee to manage risks proactively, including embracing the positive side of risk, and to communicate openly about risk.

## 2.0 Audit Objective, Scope and Approach

### 2.1 Audit Objective

The objective of this audit was to assess the effectiveness of the IRM Framework by independently validating the IRM Team's 2020 self-assessment against the 2011 Canadian Standards Association CAN/CSA-ISO-31000 Risk Management Maturity Continuum and Assessment Criteria (Maturity Continuum) and associated principles and attributes:

- Continual improvement
- Full accountability for risks
- Application of risk management in all decision making
- Continual communications
- Full integration into the organization's governance structure

### 2.2 Audit Scope

The scope of the audit included processes in operation from January 1, 2019 to November 30, 2020.

### 2.3 Audit Approach

Our audit approach included:

- Evaluating the design and operating effectiveness of the following key processes:
  - The Service Risk Register (SRR) process;
  - The Principal Corporate Risk (PCR) process; and
  - The IRM Program's Qualitative and Quantitative Assessment of SRR.
- Reviewing the IRM Policy, IRM Guidelines, reports, procedures, including those related to risk appetite and tolerance.
- Interviewing members of the IRM Team and gathering input from a sample of key stakeholders (PCR Owners, members of the Corporate Risk Network<sup>3</sup>, and members of Audit Committee).

It is our understanding the COVID-19 pandemic impacted IRM processes and activities. We adjusted our test plan to incorporate alternatives developed in response, where appropriate.

---

<sup>3</sup> Corporate Risk Network – Individual who has worked with the IRM Team and/or has been involved in risk management at The City (Departmental Planners, Business Strategists, Business Coordinators, etc.). Does not include PCR Owners or Service Owners. – who were included in interviews.



### 3.0 Results

During the planning phase of the audit, we reviewed the ISO-31000 2018 International Standard and determined the Maturity Continuum is aligned with the updated standards. The IRM Team conducted a self-assessment against the Maturity Continuum.


<b>Risk Management Maturity Continuum And Assessment Criteria</b>			
	<b>Basic</b>	<b>Enhanced</b>	<b>Excellence</b>
Risk management maturity continuum- Description	The organization meets basic internal and external stakeholder risk management expectations from primarily compliance or specialized risk management perspectives.	Activities and techniques are employed for enhanced stakeholder confidence that strategic, operational, and project risks are managed proactively. Integration of risk management activities is occurring across the organization.	Risk management is seen as an organization-wide tool to address uncertainty, aid decision making at all levels, improve organizational performance, and enhance governance and accountability. Risk management is a demonstrated core value of the organization.
<b>Risk Management Maturity Continuum</b>			
	Fledgling risk management practices	Maturing risk management practices	ISO 31000 attributes of enhanced risk management
			

Table 1<sup>4</sup>

We independently validated the IRM Team’s self-assessment against the Maturity Continuum and associated principles and attributes and determined, overall, the IRM Framework is at an enhanced level of maturity. At this level, on the maturity continuum as defined in Table 1 above, IRM practices are maturing, which provides confidence to stakeholders that strategic, operational, and project risks are managed proactively based on activities and techniques employed, and integration of risk management activities is occurring across the organization. In contrast, the results of the last IRM audit in 2014 supported a “low enhanced” level of maturity, that is, a combination of maturing and basic risk management practices. We also determined each individual attribute was at an enhanced level of maturity and included details of the IRM Team’s and our assessment in the Appendix.

<sup>4</sup> Canadian Standards Association Risk Management Maturity Continuum and Assessment Criteria as defined in the Implementation Guide to CAN/CSA-ISO 31000, Risk Management Principles and Guidelines (Q31001-11, March 2011).

The IRM Team is focused on continually advancing and improving the Framework. Our recommendations are intended to help the IRM Team achieve clarity on the direction of the Framework's maturity and identify areas where they can build on and improve current processes. Detailed test results for each attribute are included in sections 3.1-3.6 below.

### **3.1 Continuous Improvement**

In 2019 and 2020, the IRM Team implemented a number of mechanisms that contribute to continual improvement of risk management. These include:

- Implementing the annual risk maturity survey with the purpose of gathering feedback on risk management at The City, including awareness and knowledge of the IRM Policy, and the risk maturity model;
- Developing the e-learning course, which provides high level training intended to help individuals provide an understanding of risk management and includes gathering feedback from participants; and
- Implementing the SRR assessment process, which includes a quantitative and qualitative review.

The IRM Team incorporate feedback from continuous improvement mechanisms into annual work-plans, which may include consulting sessions and workshops.

#### IRM Framework Performance Assessment

There has been significant progress in the maturity of the IRM Framework, since we last completed an audit of IRM in 2014. Under ISO 31000, organizations should periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviors and determine whether it remains suitable to support achieving the objectives of the organization. We recommended the IRM Team make a collective decision with the Executive Leadership Team (ELT) on the desired level of maturity including formal input from Audit Committee, which will help them plan resources and focus improvement activities (Recommendation #1).

Various methods can be utilized to periodically evaluate performance including self-assessments, surveys and interviews. We noted that the IRM Team gather feedback from stakeholders through presentations with the ELT and Audit Committee and their annual maturity survey to the Corporate Risk Network. However, current processes to evaluate IRM Framework performance do not include formal engagement with all relevant key stakeholders. We recommended the IRM Team review current methods utilized to evaluate performance and implement processes that include feedback from relevant stakeholders (Recommendation #1).

#### IRM Program Performance Measures

The IRM Program established performance measures to track the achievement of goals. In 2020, Program goals were to develop a robust risk culture, mature The City's IRM Program and improve risk communication and coordination. We reviewed the IRM Program's seven performance measures and assessed alignment to IRM Program goals, relevance, measurability and inclusion of realistic timelines.

The IRM Team has made good progress establishing measures, which generally align to IRM Program goals. In addition, the IRM Team shared results with management, including progress on program maturity in reports to ELT in 2019 and 2020. We noted effectiveness of performance measures can be further enhanced by re-evaluating measures and setting performance targets with timelines, which will allow the IRM Team to better measure and track progress against goals. (Recommendation #3). The IRM Team has indicated in their response that they intend to align timelines to Results Based Accountability practices, which is the City's adopted framework for performance.

#### Service Risk Register Assessment Process

The SRR assessment process was established in 2019 to evaluate the quantity and quality of individual SRR. The quantitative review provides insight on the number of risks, risk ratings and trends from year to year, such as the distribution of risks into high, medium and low, and the number of risks requiring significant improvement. Twice a year, the IRM Team also complete a qualitative assessment that rates each SRR submission based on six criteria, then review results and identify improvements. Qualitative results inform the Work-Plan by identifying where to focus training and consulting activities.

In addition, the IRM Team indicated they complete a summary of findings and trends as an input into the one-page evidence based summaries that are completed for the PCR process.

Although we determined the qualitative assessment process contributes to improved SRR quality and risk management, our review of design and operating effectiveness identified enhancements to further support consistent rating and the implementation of improvements identified by communicating improvements to employees responsible for completing the SRR (Recommendation #4).

### **3.2 Full Accountability for Risks**

To validate the IRM Team's assessment, we reviewed the IRM Policy and Administrative Guidelines, the SRR and PCR processes and conducted interviews with a sample of key stakeholders as detailed below.

#### IRM Policy and Administrative Guidelines

On February 3, 2020, the IRM Policy (CC001) was amended to reflect the opportunity to capitalize on risk and create a culture that embraces the appropriate levels of risk. Amendments aligned with the ISO 31000:2018 International Standard, which is the foundation of The City's IRM Framework.

In addition, the IRM Team developed Administrative Guidelines (ALT2020-1109), which ELT approved in November 2020. The purpose of these guidelines is to operationalize the IRM Council Policy, outline Administration's leadership commitment on the importance of managing risk at The City, and create consistency in risk management practices.

We reviewed the IRM Policy and Administrative Guidelines and determined roles and responsibilities are appropriately assigned to Council, senior management, Administration and all other employees and clear reporting lines are established.

Service Risk Register Process

We reviewed the SRR process and determined it is a well-established bi-annual process that is operating effectively to identify, analyze and evaluate risks. We noted the IRM Team implemented the 5x5 Risk Matrix (heat map) in 2019, to enhance the risk assessment process. We confirmed, through interviews, that services review, update and approve SRR before they are submitted to the IRM Team.

We interviewed a sample of 25 individuals in the Corporate Risk Network who indicated they had the appropriate resources, skills and knowledge, and understanding of controls and the foundational tools to complete the SRR. They noted the IRM Team provide good support, is helpful and knowledgeable about processes and easy to engage with, and provide information on SRR completion through emails, training and workshops. Stakeholders interviewed also identified the following opportunities for improvement: facilitate peer learning, offer coaching on conversations with managers on risk, and provide more tactical examples of risk management in training and consulting sessions. The IRM Team could consider implementing these opportunities in future work-plans.

The risk register process transitioned to a service line approach in 2019 as part of One Calgary 2019-2022 Service Plans and Budgets. We analyzed IRM Program data and noted services made progress towards submitting individual SRR rather than SRR combined by business unit. We confirmed between 2019 and 2020, submission<sup>5</sup> rates were between 95% and 98%, with the exception of mid-year 2020 submissions. At mid-year 2020, submissions declined to 52%, which was directly linked to resource constraints within services due to The City's response to the COVID-19 pandemic. The IRM Team successfully leveraged other sources including One Calgary monthly submissions, to obtain information on risks and risk analysis within those service lines. This decision was made considering the capacity of the organization and the importance of collecting risk information.

We also noted through a review of the service lines submitted that, although the IRM Team follow up with service lines that do not submit an SRR, there is no escalation process to ensure the SRR was received. We recommended that instances where an SRR has not been submitted should be escalated for resolution to support effective risk management and provide valuable information to the IRM Team to support the PCR process and continual improvement (Recommendation #5).

---

<sup>5</sup> In a combined or individual format.

Principal Corporate Risk Process

The corporate risk review process to confirm and update PCR utilizes a bottom up and top down approach, which is outlined in the following diagram.

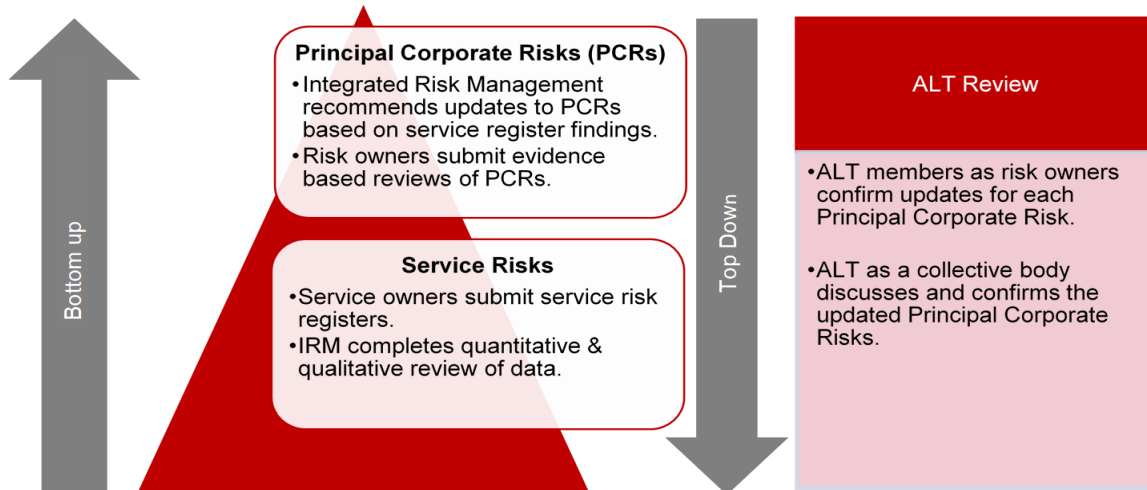


Diagram 1<sup>6</sup>

We reviewed the PCR process and determined it is operating effectively as designed. The IRM Team analyze the PCR and meet with risk owners and/or their delegates to discuss updates. Risk owners and/or their delegates prepare evidence based one-page summaries for each PCR. The IRM Team review each PCR summary, since these directly inform the bi-annual reports to ELT. PCR owners confirmed in interviews they discuss, review and approve evidence based summaries before they are sent to the IRM Team. They also indicated that external factors are considered in the summaries since many PCR are heavily influenced by external factors.

We reviewed 2019 and 2020 bi-annual reports provided to ELT and associated minutes and noted ELT approved updates to PCR, which included changes to PCR from period to period. PCR owners confirmed ELT collectively discuss PCR results and changes.

**3.3 Application of Risk Management in all Decisions**

PCR Owners interviewed indicated risk is inherently embedded into all ELT and departmental decisions and there has been significant improvement in the quality of risk analysis. In addition, the majority indicated they have the foundational tools to make appropriate decisions and the application of risk management was reflected in ELT and Council reports. Interviewees indicated the quality and sophistication of risk analysis in discussions, and Council and Committee reports has improved.

Audit Committee members interviewed indicated that consideration of risk and the application of risk management is appropriately reflected in reports brought forward to Council. Members of Audit Committee commented there is good risk awareness at The City and a good risk culture.

<sup>6</sup> Corporate Risk Review Process- ALT2019-0355 Attachment 1

Although the IRM Framework meets enhanced attributes (see Appendix), if a decision is made to further advance the maturity of risk management (see Section 3.1), there is an opportunity to provide guidance on a more structured approach (formal, intentional and consistent) to incorporate risk management into ELT and departmental decision making and guidance on decision making that applies to day-to-day operations.

### **3.4 Continual Communications**

The IRM Team developed a 2020 communication plan targeted to two audiences, key stakeholders involved in the SRR and PCR processes, and all employees. The 2020 plan included the following goals, which align to IRM Program goals:

- Create awareness of risk management at The City with key stakeholders; and
- Facilitate well-coordinated and ongoing communications to all employees about risk management to enhance the risk culture and maturity at The City.

The tactical communication plan for key stakeholders includes semi-annual corporate communication on SRR and PCR deadlines and information on tools and resources, which is shared through emails, meetings, the myCity IRM internal webpage, and the corporate risk reports presented to ELT and Audit Committee. The communication plan to all employees highlights the importance of risk management through All Employee and Take Five emails, myCity articles, and IRM Program website updates.

The IRM Team is doing a good job of identifying and providing information to key stakeholders and all employees. Based on our review, planned communication to key stakeholders and all employees is occurring. We also confirmed the IRM Team provided semi-annual reports to ELT and Audit Committee in 2019 and 2020.

In interviews with key stakeholders, they identified opportunities to utilize plain language and provide tactical examples of day-to-day risk management, including success stories in future communication. The IRM Team created a common language/definitions guide for a strategic session with General Managers in May 2020, which they are considering finalizing.

### **3.5 Integration**

Principles of integrated risk management are outlined in the IRM Policy, including recognition that risk management is an essential component of good management and the expectation that risk management is integrated into existing long term strategic and business planning as well as informed decision-making in the day-to-day management of activities. In addition, IRM Administrative Guidelines indicate City projects are required to identify, assess and treat risk.

We observed Administration has incorporated risk management into One Calgary 2019-2022 Business Plans and Budgets, and in particular the 2020 Mid-Cycle Adjustments. In addition, Administration has incorporated risk management into other work such as the Solutions for Achieving Value and Excellence Program and monthly reports to Council on the service and financial impacts of COVID-19.

PCR owners interviewed indicated integration of IRM into all City management processes is improving and generally there is a good understanding of the IRM Framework, the IRM Policy, tools and templates, and responsibilities.

Although efforts are under way to ensure risk management is viewed as central to the organization's management processes there is an opportunity to further advance the maturity of this attribute based on direction from ELT on desired level of maturity (see Section 3.1). We are sharing the following opportunities identified by key stakeholders interviewed for the IRM Team's consideration: identify where there are still silos or groups whose processes do not align with IRM practices, and increase cross-corporate collaboration.

### **3.6 Risk Appetite and Tolerance**

Although risk appetite and tolerance is not a specific attribute outlined in the Maturity Continuum, we determined that this was an important component of risk management to review since the IRM Policy includes specific requirements of all employees with respect to risk appetite and tolerance.

The IRM Team is working on advancing risk appetite and tolerance. They have worked directly with business units through consulting sessions, and developed Risk Appetite Guidelines to provide a common understanding of risk appetite and tolerance as well as common framework for implementing. However, there is limited guidance on approved risk appetite and tolerance levels. We recommended the IRM Team expand on current guidance and raise awareness to support employee roles and responsibilities in risk management outlined in the IRM Policy (Recommendation#2).

We would like to thank the IRM Team and the members of Audit Committee, PCR Owners and members of the Service Risk Network, who participated in interviews, for their assistance and support throughout this audit.

## 4.0 Observations and Recommendations

### 4.1 IRM Framework Performance Assessment

Current IRM processes used to evaluate the effectiveness of the IRM Framework do not include formal engagement with all relevant City stakeholders. The IRM Program should periodically evaluate the framework and identify strengths, successes, gaps and areas for improvement. Evaluations should include relevant stakeholders at all levels to provide feedback and direction to the IRM Program to support planning and the effective utilization of resources.

The City's IRM Framework is based on the ISO 31000 Risk Management Standards. ISO 31000-2018 Risk Management Guidelines indicate an organization should periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviors and determine whether it remains suitable to support achieving the objectives of the organization.

As a first step, the IRM team should gather formal feedback from ELT and Audit Committee (in keeping with the Audit Committee's role with regard to risk management outlined in Bylaw 33M2020- Bylaw to Continue the Audit Committee) on expectations of risk maturity of the IRM Framework, and then make a decision with ELT, on desired level of maturity. Since the IRM Program contributes to The City's risk maturity, clear expectations will help to plan resources and focus improvement activities. We interviewed six PCR owners who echoed that an important first step for the IRM Team to be successful, was to be clear on maturity expectations.

Various methods can be utilized to periodically evaluate the risk management framework. The IRM Team conducted a self-assessment against the Maturity Continuum for the purpose of this audit using a three-point scale. However, the IRM Team do not regularly complete this type of formal self-assessment.

Currently, the IRM Team conduct an annual survey (implemented in 2019), to gather feedback on risk management at The City, including awareness and knowledge of the IRM Policy, the risk maturity model and information on continuous improvement efforts. The survey uses the Archer Governance Risk and Control 5-point scale maturity model. Information gathered informs the IRM Program's annual work-plan and helps the IRM Team advance the maturity of IRM. The survey is sent to individuals familiar with risk management at The City, however, the list of survey recipients does not include PCR Owners or all Service Owners and/or delegates.

Although the IRM Team noted they engage ELT and Audit Committee members through one-on-one interviews and meetings, emails, as well as on feedback on reports on risk maturity presented to ELT and Audit Committee, there is an opportunity to be more intentional. The IRM Team should implement processes to obtain formal input and direction on the performance of the IRM Framework from relevant stakeholders.

The IRM Team could expand the annual survey to include relevant stakeholders at all levels of the organization or utilize the current survey along with one or more other methods to evaluate the framework. If committed to a maturity model approach, the IRM Team should



determine the most appropriate maturity model (Maturity Continuum, Archer or others) to utilize for formal assessments.

**Recommendation #1**

The Leader Performance Measurement, Benchmarking and Risk:

- Direct the IRM Team to make a collective decision with the ELT on the desired level of maturity, which will include further engagement with Audit Committee;
- Review current methods utilized to evaluate IRM Framework performance and implement processes that include a standard approach for obtaining feedback from relevant stakeholders at all levels of The City; and
- Determine the appropriate model upon which to base the evaluation of the IRM Framework.

**Management Response**

Agreed.

Action Plan	Responsibility
<p>IRM will consult with the Executive Leadership Team and the Audit Committee (in keeping with the Audit Committee’s role with regard to risk management outlined in Bylaw 33M2020- Bylaw Continue the Audit Committee) to determine the desired level of maturity and frequency of review of the IRM Framework. Based on the desired results, IRM will review current methods and implement processes that include feedback from stakeholders at all levels of The City. This includes utilizing maturity models appropriate to stakeholder needs.</p>	<p><u>Lead:</u> Manager, Corporate Initiatives; Team Lead, PMBR</p> <p><u>Support:</u> IRM Team, Executive Leadership Team (ELT)</p> <p><u>Commitment Date:</u> December 31, 2022</p>

**4.2 IRM Risk Appetite and Tolerance**

Although the IRM Team developed Risk Appetite and Tolerance Guidelines, there is limited guidance on approved risk appetite and tolerance levels. The IRM Program should provide detailed guidelines that support effective employee decision making.

The IRM Policy (CC011) states: “All City employees are responsible for managing risks within their respective areas.” The Policy also indicates: “All employees of The City will accept an appropriate level of risk defined by approved risk appetite levels.” and “All employees of The City will operate within approved risk tolerance levels.”

The IRM Team developed guidelines to provide The City with a common understanding of risk appetite and tolerance as well as a common framework for implementing. The guidelines utilize a 1-5 risk appetite scale and sort the PCRs into six risk types. Further guidance on risk appetite for each PCR was provided in AC2020-0711 Attachment 3, which plotted each PCR on the risk appetite scale. However, guidance does not include risk appetite for operational

risks within the organization and guidance on risk tolerance is limited to instances where the IRM Team has worked directly with a specific business unit through consulting sessions. Members of the Corporate Risk Network, PCR owners, and Audit Committee also indicated in interviews that further clarification and guidance on how to apply risk appetite and tolerance would be beneficial to enhance decision making within the City and that guidelines should be circulated to appropriate City staff.

We also reviewed a sample of five ELT reports from 2019 and 2020 and noted consideration of risk appetite/tolerance was not included in these reports. Including this information would further support effective decision making. We were advised through interviews with PCR Owners that a review of reports to ELT will occur in 2021.

The IRM Team participated in a review of Council reports in September 2020 that resulted in an update to the templates however, information on risk appetite and tolerance was not included in the report template. Further updates to the templates should consider guidance on risk appetite and tolerance.

### Recommendation #2

The Leader Performance Measurement, Benchmarking and Risk:

- Expand on current Risk Appetite and Tolerance Guidelines to include approved levels for both strategic and operational risk to support effective decision making within The City;
- Raise awareness of approved risk appetite and tolerance levels through communication and training; and
- Provide guidance/direction on how including risk appetite/tolerance should be considered in reports to ELT and Council (if future updates occur).

Management Response

Agreed.

Action Plan	Responsibility
<p>In accordance with the direction received from the Executive Leadership Team (ELT) and Audit Committee, regarding the desired level of risk maturity, IRM will expand on the Risk Appetite and Tolerance guidelines for both strategic and operational risk. This work is in keeping with the recent updates to the IRM Policy and the approved IRM Guidelines and is dependent upon the direction from the ELT regarding desired level of maturity. If there is a desire to move towards excellence, broader organizational resources will be required to support collaboration and cultural change.</p> <p>A measured and pragmatic approach to Risk Appetite and Tolerance is recommended to ensure that guidance and tools are appropriate to support strategic and operational risk. Given that leading practice for municipal environments is limited, implementation of this initiative will require analysis, testing and refinement prior to the broader roll-out to the organization.</p>	<p><u>Lead:</u> Manager, Corporate Initiatives; Team Lead, PMBR</p> <p><u>Support:</u> IRM Team, Executive Leadership Team, Service Owners.</p> <p><u>Commitment Date:</u> December 31, 2022</p>

**4.3 Performance Measures**

IRM Program performance measures can be enhanced to ensure progress towards IRM Program goals can be effectively measured. Performance measures should be specific, measurable, achievable, relevant and timely (SMART).

IRM Program goals in 2020 were to develop a robust risk culture, mature The City’s IRM Program, and improve risk communication and coordination. We reviewed the IRM Program’s seven performance measures and noted effectiveness can be enhanced by re-evaluating targets and setting timelines for risk maturity, and setting performance targets and timelines for the remaining measures which will allow the IRM Team to better track progress against goals. In addition, measures should be re-evaluated to ensure they are relevant, which is detailed below along with general descriptions:

1. Risks Identified - Tracks the number of risks identified, which does not provide the IRM Team with information on achieving program goals. The IRM Team should consider alternate measures based on trends identified through the quantitative assessment process, which includes % risks rated medium, high or extensive, % of increasing service risk, % of risks requiring significant improvement.
2. Qualitative Risk Ratings - Tracks overall qualitative assessment ratings for the six criteria . The IRM Team should consider using % of SRR with scores below 3 rather than averages to provide better insight on the quality of SRR.

3. City-Specific Learning (IRM E-Course) - Measures overall satisfaction and applicability of learning to workplace.
4. Risk Maturity - Tracks average risk maturity rating determined by stakeholder survey. The IRM Team indicated a target of 4 with a timeline of 2022. The IRM Team should re-evaluate the target and timeline based on additional feedback on desired level of maturity noted under Recommendation #1.
5. Consulting - Tracks the number of internal consulting sessions as an indicator of risk culture advancement.
6. Communications - Tracks the number of communications compared to prior year as a measure of the IRM Teams' intention to communicate more. Although the focus is on "how much", the IRM Team is planning on building in a measure of "is anyone better off", which will improve the relevance of this measure.
7. Reporting - The IRM Team track the number of reports they wrote or contributed to. The IRM Team should re-evaluate this measure since it does not provide information on achieving IRM Program goals.

**Recommendation #3**

The Leader Performance Measurement, Benchmarking and Risk re-evaluate current performance measures and ensure they are specific, measurable, attainable, relevant, and time oriented (SMART).

**Management Response**

Agreed.

Action Plan	Responsibility
<p>IRM is currently re-evaluating current performance measures as part of the 2021 work plan. Progress is being made to align performance measures with IRM goals and results in keeping with Results Based Accountability, The City's adopted framework for performance measurement.</p> <p>The identification of performance measures takes time and includes refinement of measures, collection of data, analysis and reporting. Given the resources and time required, the updates to measures will align with the development of measures for the next business plan cycle (2023-2026).</p>	<p><u>Lead:</u> Team Lead, PMBR</p> <p><u>Support:</u> IRM Team</p> <p><u>Commitment Date:</u> December 31, 2022</p>

**4.4 Service Risk Register Assessment Process**

The design of the SRR qualitative assessment process can be enhanced to support consistent rating, and improvement in the quality of SRR submitted. An effective process ensures the IRM Team is able to consistently identify services in need of assistance, and support improvements in SRR quality and value from year to year.

The qualitative assessment process was established in 2019 to evaluate the quality of individual SRR. Results inform the IRM Program's work-plan by identifying where to focus communications, training and consulting activities, and inform the PCR process.

Once the SRRs are received (twice per year), the IRM Team divide them amongst the team for evaluation. The IRM Team developed qualitative analysis criteria, which include six criteria that are assigned an individual rating from 1 to 5. Once the IRM Team evaluate the SRR, they provide comments on the overall rating. SRR that score less than 3 are considered to be in need of assistance. The IRM Team then meet to review results and identify improvements. The IRM Team also calculate an overall SRR rating for performance measure purposes.

Following the assessment, the IRM Team meet with service owners including department representatives to discuss common themes for improvement. However, interviewees indicated information from these meetings is often not being cascaded back down to the individuals responsible for completing the SRR.

We reviewed the rating criteria and noted they were based on reasonable measures to assess SRR quality since they included a review of risks, indicators, ratings and responses, and overall alignment. However, criteria are subjective and rely on the experience and knowledge of the IRM Team to complete individual scoring. Although, for the most part there has been a consistent team with knowledge and expertise in IRM evaluating the SRR, the consistency of the process can be enhanced by adding comments with the rationale for each rating.

We reviewed the methodology to assign an overall rating to each criteria and noted in 2019, the IRM Team used a weighted rating while in 2020 they used an average rating. The methodology should be consistent to ensure performance can be effectively evaluated from year to year. We also noted one service did not receive an overall score in 2019.

#### Recommendation #4

The Leader Performance Measurement, Benchmarking and Risk enhance the SRR qualitative assessment process by:

- Communicating improvements identified to employees responsible for completing the SRR;
- Establishing and documenting a consistent methodology to assign an overall rating; and
- Adding comments to each of the six criteria rated, to support rating consistency from year to year.

Management Response

Agreed.

Action Plan	Responsibility
<p>Enhancements to the SRR qualitative assessment process are underway to support improvements in SRR quality and value from year to year. Enhancements include: informing the people who complete the SRR as to the specific aspect being focused on for improvement; engaging about the overall results of the Corporate Risk Review process; providing assessment criteria and guidelines to the risk register evaluators to improve consistency in the qualitative review process; and requiring the evaluators to provide comments on their ratings of the risk registers.</p>	<p><u>Lead:</u> Team Lead, PMBR</p> <p><u>Support:</u> IRM Team, Service Owners and Teams</p> <p><u>Commitment Date:</u> December 31, 2021</p>

**4.5 Service Risk Register Process**

Although the IRM Team review SRR received and follow-up with services that do not submit, there is no escalation process to ensure SRR are submitted. All City services that report to Administration are required to submit an SRR to support effective risk management and provide valuable information to the IRM Team to support the PCR process and continual improvement.

We analyzed IRM Program data and noted the majority of services submitted an SRR in 2019 and at year-end 2020. Although we noted evidence of follow-up to obtain missing SRR, the IRM Team advised there was no escalation process to ensure information was received.

Recommendation #5

The Leader Performance Measurement, Benchmarking and Risk escalate instances where an SRR is not submitted for resolution in keeping with the IRM Administrative Guidelines approved by ELT in 2020 November.

Management Response

Agreed.

Action Plan	Responsibility
<p>In keeping with the Integrated Risk Management (IRM) Guidelines services are required to complete and submit a Service Risk Register (SRR). The City conducts at least two cross-corporate risk reviews annually. At a minimum, this review includes an analysis of SRR completed by services and an evidence-based analysis of Principal Corporate Risks by Principal Corporate Risk owners.</p> <p>For instances when an SRR is not submitted, there should be an escalation process to understand the circumstances and to determine the best course of action to resolve the issue. IRM will develop an escalation process to support effective risk management and to ensure that valuable information is provided to the IRM team to support the PCR process and continual improvement.</p>	<p><u>Lead</u>: Team Lead, PMBR</p> <p><u>Support</u>: IRM Team, Service Owners and Teams.</p> <p><u>Commitment Date</u>: December 31, 2021</p>

## Appendix

### Maturity Continuum Assessment

Attribute	CAN/CSA-ISO 31000 Principles	Enhanced Attributes	Assessment
<b>Continual improvement</b>	Organizations should develop and implement strategies to improve their risk management maturity alongside other aspects of their organization.	<p>Frequent risk assessments occur in line with normal management analysis and reporting. Risks are assessed and managed in an integrated fashion across the strategic, operational, and project levels of an organization.</p> <p>Explicit requirements are being defined for risk management performance assessment to align it with the governance and accountability structure.</p> <p>An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review, and subsequent modification of processes, systems, resources, capability and skill.</p>	<p>IRM Team-Low-Excellence</p> <p>Audit-Enhanced</p>
<b>Full accountability for risks</b>	<p>Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization.</p> <p>Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.</p> <p>Risk management recognizes the capabilities, perceptions, and intentions of external and internal</p>	<p>Efforts are under way to ensure that risk management includes comprehensive, fully defined, and fully accepted accountability for risks, controls, and risk treatment tasks.</p> <p>Designated individuals fully accept accountability, are appropriately skilled, and have adequate resources to check controls, monitor risks, improve controls, and communicate effectively about risks and their management to external and internal stakeholders.</p>	<p>IRM Team-Enhanced</p> <p>Audit-Enhanced</p>



Attribute	CAN/CSA-ISO 31000 Principles	Enhanced Attributes	Assessment
	<p>people who can facilitate or hinder achievement of the organization's objectives.</p>		
<p><b>Application of risk management in all decision making</b></p>	<p>Risk management helps decision makers make informed choices, prioritize actions, and distinguish among alternative courses of action.</p> <p>Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.</p> <p>The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgement. However, decision makers should inform themselves of, and take into account, any limitations of the data or modelling used or the possibility of divergence among experts.</p>	<p>Efforts are under way to ensure that all decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management in a systematic, structured, and timely manner. This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place.</p> <p>Major capital, operational, technology, and change management decisions are beginning to be supported by the best available risk assessments. Risk and control activities are being embedded in business processes.</p>	<p>IRM Team-Enhanced</p> <p>Audit-Enhanced</p>
<p><b>Full integration into the organization's governance structure</b></p>	<p>Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.</p> <p>Risk management is aligned with the organization's external and internal context and risk profile.</p> <p>A systematic, timely, and structured approach to risk management contributes to efficiency and to consistent, comparable, and reliable results.</p>	<p>Efforts are under way to ensure risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives.</p> <p>The governance structure and process have been refined and are based on the management of risk.</p> <p>Efforts are under way at the management level to ensure that risk management fully supports the achievement of objectives. This includes enhancement of the decision-making processes and risk-based culture of the organization.</p>	<p>IRM Team-Enhanced</p> <p>Audit-Enhanced</p>

Attribute	CAN/CSA-ISO 31000 Principles	Enhanced Attributes	Assessment
<p><b>Continual communications</b></p>	<p>Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.</p> <p>Risk management continually identifies and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.</p>	<p>Efforts are under way to develop and implement enhanced risk management continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.</p> <p>Efforts are under way to provide comprehensive reporting to the Board of Directors or governing body, the audit committee, and key stakeholders on current risk levels and future risk issues.</p>	<p>IRM Team-Enhanced</p> <p>Audit-Enhanced</p>