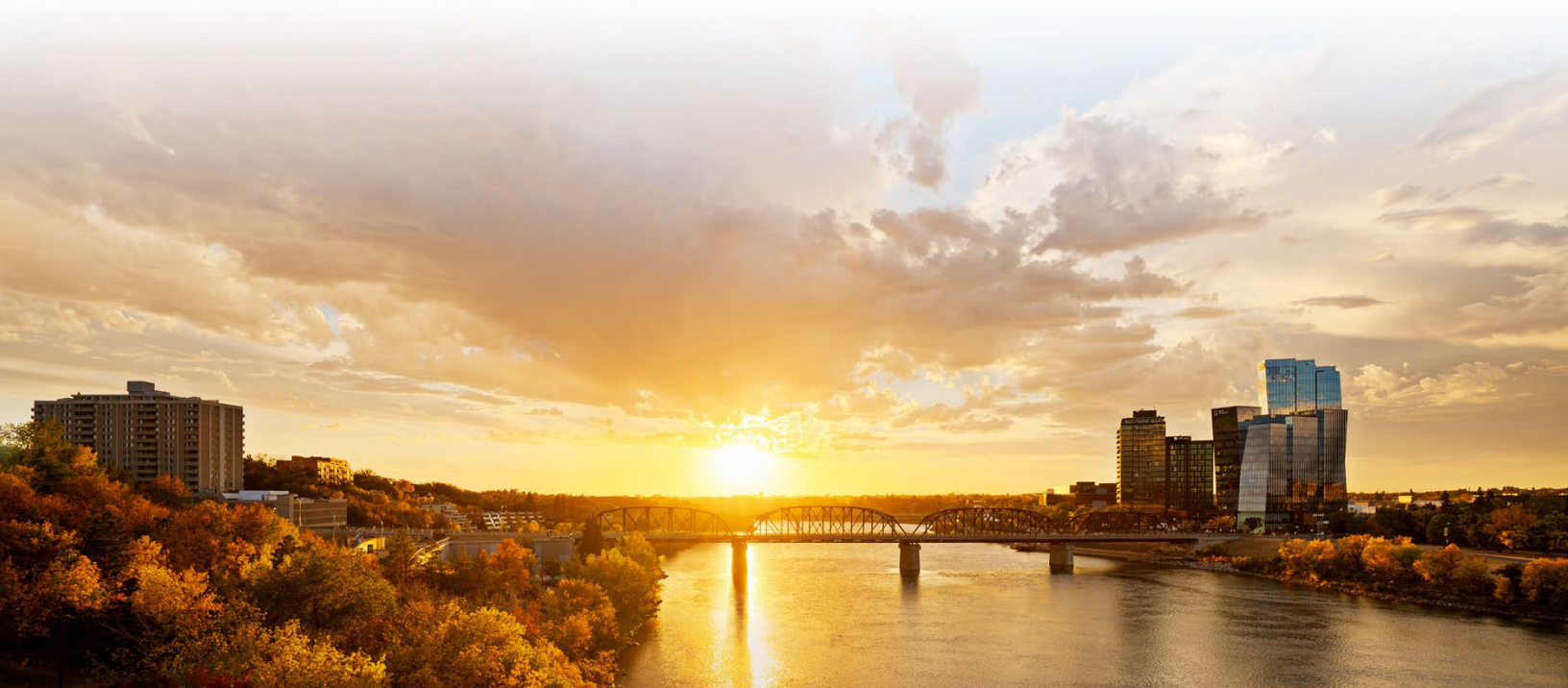
City of Saskatoon

RISK MANAGEMENT PROGRAM AUDIT

Terms of Reference

Independent Office of the City Auditor

May 7, 2025



TERMS OF REFERENCE

Background

The City's Risk Based Management Program (Program) was established in 2014 through the approval of Council Policy C02-040 *Corporate Governance – Risk Based Management*. Section 3.2 of the Policy called for Administration to "embed into corporate operations and reporting a systematic, proactive and ongoing process to understand and manage risk and uncertainty, and to communicate risk information throughout the City of Saskatoon (City), which will contribute positively to the achievement of corporate objectives."

The Program is based on the "internationally-accepted principles and guidelines for risk management[1]" as set out in ISO 31000 *Risk management – Guidelines*. A visualization of the risk management methodology is included in Appendix A.

In accordance with the approved 2025-2026 Audit Plan, the Independent Office of the City Auditor (Office) has initiated the audit of the Program.

Objective

The objective of the audit is to assess the maturity of the Risk Management Program based on the following five dimensions identified in the Enterprise Risk Management (ERM) Assessment Model developed by Ayse Nordal and Ole Martin Kjørstad[2]:

- Risk management, strategy and decision-making processes.
- Communication, information and reporting.
- Organization, authority and interaction.
- IT-tools and analyses.
- Framework and processes.

There are many risk management maturity models available. The Nordal & Kjørstad model was selected, in conjunction with the Corporate Risk Manager, as it:

- Is a simplified model with clearly defined and easy to understand criterion.
- Allows for a separate assessment on five dimensions and acknowledges that organizations can be/aspire to be at different levels for each.
- Is not framework specific but rather is a compilation of practices that are common in well-known frameworks.

The model includes a maturity goal and 10 assessment criteria for each dimension, a summary of which is included in Appendix B.

---

[1] ISO 31000:2018 *Risk management – Guidelines*. https://www.iso.org/standard/65694.html
[2] ERM Assessment Model, Nordal & Kjørstad (2017) https://iia.no/product/modenhetsmodell-risikostyring/

Scope

The scope includes a review of the current state of the Program including policies, processes, risk registers and other relevant documentations available at the time of the audit. The audit will include the functions performed by the Corporate Risk Manager as well as the application of the Program by the senior leaders across the City.

The scope does not include:

- Risk management activities related to the independent boards and corporations.
- Assurance over the effectiveness of mitigation strategies related to specific risks identified in the Risk Management Program.
- An assessment of conformance to the ISO 31000 Risk management – Guidelines.

Approach

The audit will be performed by the City Auditor and Senior Audit Specialist. The maturity assessment will be performed using a combination of procedures such as:

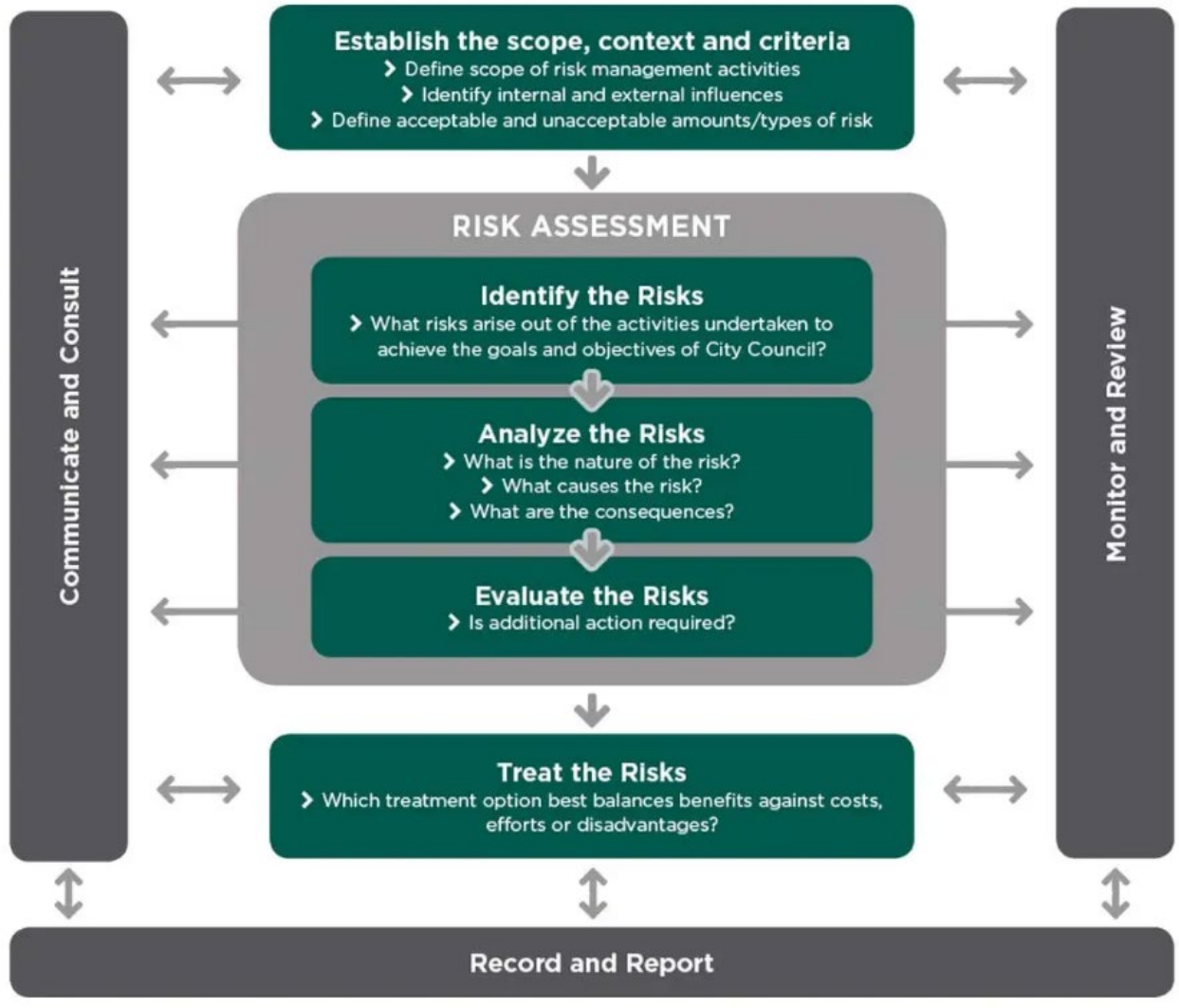
- Review of Program documentation.
- Interviews with executive leadership and Corporate Risk Manager.
- Surveys of department directors and other key personnel.
- Comparative analysis with similar municipalities and/or other government entities, contingent on availability of information.

Deliverables

The audit report will include the results of the maturity assessment highlighting strengths of the Program along with recommendations related to potential areas of improvement. The draft audit report will be presented to Administration for review and comment prior to finalization. The final audit report will be presented to the Standing Policy Committee on Finance and is expected to be complete in Q3 2025.

APPENDICES

Appendix A – ISO 31000 Risk Management Process



Source: Corporate Risk 2018 Annual Report (page 6) https://www.saskatoon.ca/sites/default/files/documents/corporaterisk-2018ar_-_web_version.pdf, adapted from ISO 31000:2018 Risk management – Guidelines.

Appendix B – ERM Assessment Model, Nordal & Kjørstad (2017)

The model includes five dimensions each with a maturity goal and 10 assessment criteria. The following table includes the dimensions, corresponding maturity goals and a summary of the assessment criteria for each dimension.

Dimension #1	**Risk management, strategy and decision-making processes**
Maturity Goal	Key decisions (strategic, tactical and operational) are based on a documented assessment of risk and opportunities.
Summary of Assessment Criteria	• Risk appetite is clearly defined, reflected in policies and implemented. • Risk assessments are integrated in strategy and project management and documented to support decision-making. • Assessment of uncertainty is a factor for resource allocation. • Risk management function is involved in decision making and management forums.

Dimension #2	**Communication, information and reporting**
Maturity Goal	The organization ensures regular communication and reporting of relevant information, with appropriate frequency.
Summary of Assessment Criteria	• Responsibility and ownership of risk management process, risks, actions and projects is defined and available. • Decision makers have access to updated risk information and status for ongoing actions, improvement and development measures. • Timely, accurate, relevant and reliable communication of risk information from front-line to senior/executive leadership and City Council. • Corporate Risk Manager regularly reports to/has access to City Council.

Dimension #3	**Organization, authority and interaction**
Maturity Goal	The risk management function has an appropriate organization and resource allocation.
Summary of Assessment Criteria	• Administration acknowledges their responsibility for risk management. • Risk management function has a defined mandate aligned with strategy and supported by Executive. • Risk culture and a common terminology for risk management. • Corporate Risk Manager has the necessary authority, reporting lines, relationships, access, resources and position requirements.

Dimension #4	**IT-tools and analyses**
Maturity Goal	Risk management is based on the best available information and is appropriate to the organization's needs.
Summary of Assessment Criteria	• Appropriate tools, knowledge and use of the tools, to facilitate and document risk management process. • Consistent use of tools allows for comparisons across the City. • Systems can handle sensitive data, monitor risks, and produce reports. • Appropriate channels and tools for the reporting of events.

Dimension #5	**Framework and processes**
Maturity Goal	The organization has implemented an effective and appropriate risk management framework.
Summary of Assessment Criteria	• Risk management is an iterative process, and the framework is regularly evaluated and subject to continual improvement. • Assessment models for likelihood and impact defined. • Risk management is an inclusive function and is embedded and integrated in all processes and functions. • Framework includes a system for setting priorities, monitoring and assessing effectiveness of actions and improvement initiatives.

Source: Adapted from ERM Assessment Model v 2.0, Nordal & Kjørstad (2017)
https://iia.no/product/modenhetsmodell-risikostyring/