City of
Saskatoon

RISK MANAGEMENT PROGRAM AUDIT

Audit Report

Independent Office of the City Auditor

October 8, 2025

CONTENTS

EXECUTIVE SUMMARY

Background

The 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 2025-26 Audit Plan and the Terms of Reference dated May 7, 2025, the Independent Office of the City Auditor (Office) conducted an audit of the Program.

Objective and Scope

The objective of the audit was to assess the maturity of the Program based on the Enterprise Risk Management (ERM) Assessment Model developed by Ayse Nordal and Ole Martin Kjørstad[2], which was selected in conjunction with the Corporate Risk Manager.

The scope included a current state review of the Program including policies, processes, risk registers and other relevant documentation available at the time of the audit. The scope did 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 Program.
- An assessment of conformance to the ISO 31000 Risk management – Guidelines.

Approach

The audit was performed by the City Auditor and Senior Audit Specialist and included a combination of procedures including:

- Review of Program documentation (ex. policies, toolkit, templates, risk registers, reports).
- Interviews with each of the 12 Executive Leadership Team (ELT) members and the Corporate Risk Manager.
- Survey of department directors, resulting in 34 responses (~83% of director positions).

---

[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

- Comparative analysis with three other Canadian municipalities and four provincial government-related organizations. A summary of the seven responses received is included in Appendix B and incorporated into the audit findings where relevant.
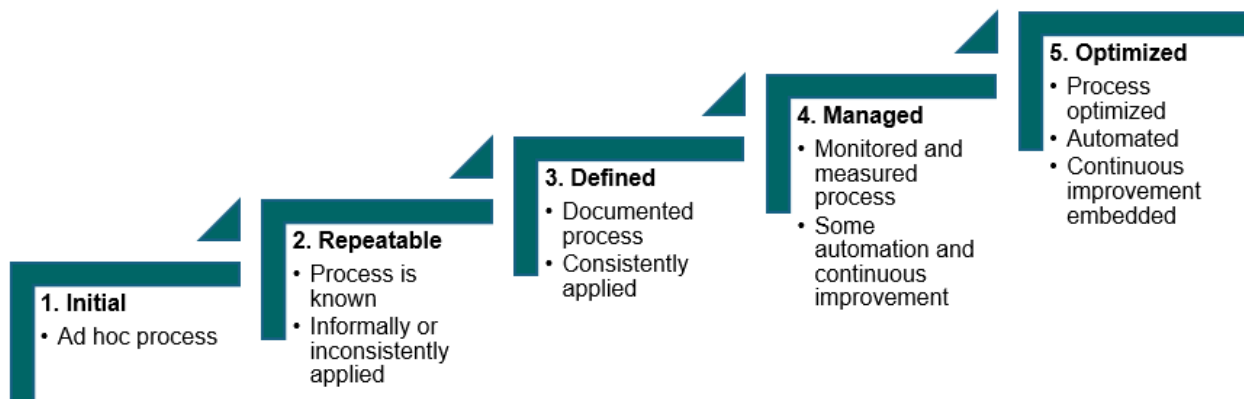
Maturity Assessment

The ERM Assessment Model (Model) assesses maturity across the following five dimensions:

- Risk management, Strategy and Decision-Making Processes
- Communication, Information and Reporting
- Organization, Authority and Interaction
- IT-tools and Analyses
- Framework and Process

Each dimension has a maturity goal and 10 assessment criteria, which are summarized in the corresponding five sections of the Detailed Report.

The Model uses a five-point maturity scale based on the number of criteria that are determined to be met. Although the Model does not define the five maturity levels, it would be reasonable to apply common maturity model descriptions such as the following:

The maturity assessment was based on review of the Corporate Risk Manager's detailed response to the Model's criteria and current Program documentation, along with insights gathered from ELT interviews, a structured survey of Directors, discussions with the Corporate Risk Manager, and information gathered from external organizations. The synthesis of this information, along with the professional judgment of the Office, informed the maturity assessment results and corresponding audit findings.

The diagram on the following page depicts the results of the Model with blue representing the current maturity level and green representing the potential future target level. The Program has a maturity level of two (Repeatable) in all dimensions except for IT-tools and Analyses which was assessed as level one (Initial). Based on the responses to the Model criteria, the target maturity level for all five dimensions has been set at four (Managed). This target maturity level is achievable if the recommendations found in the Detailed Report are fully implemented.

City of
Saskatoon
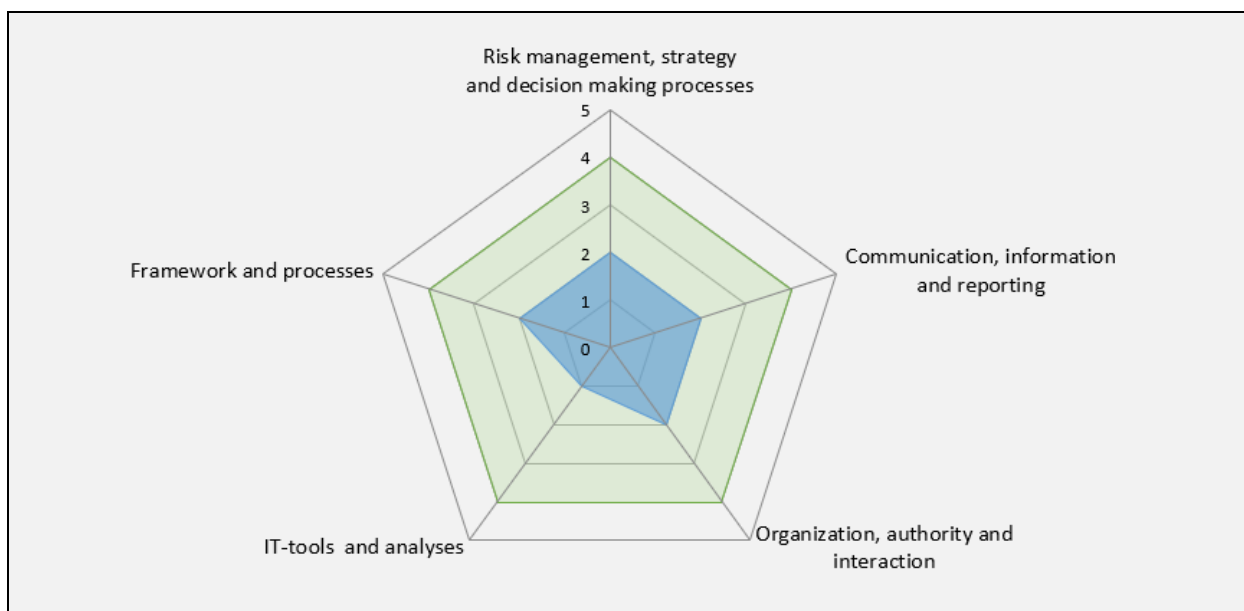
Summary of Findings

The following table summarizes the findings stemming from the maturity assessment, organized by the Model's five dimensions. More details, including the Administration's responses, are in the Detailed Report. Risk ratings are based on the guidance in Appendix C.

Dimension	Risk	Key Findings
Risk Management, Strategy and Decision-Making Processes	Medium	**1. Risk Appetite:** The City's Risk Appetite has been defined, ELT and Directors are aware of it, and it is informally considered during decision-making, but it requires periodic review and monitoring.
	Medium	**2. Strategic Alignment, Integration and Documentation:** Recent efforts have been made to align the risk and strategy functions, including a reorganization of the reporting structure. Opportunities exist to further integrate and formalize risk into decision-making, policy development and strategic planning.
Communication, Information and Reporting	High	**3. Risk Information and Reporting:** Risk information is embedded into regular discussions and reporting such as City Council and Committee reports and the Operating Budget. However, there is a lack of centralized risk repository and overall risk reporting to facilitate oversight.
Organization, Authority and Interaction	High	**4. Risk Management Oversight:** Responsibilities are outlined in various documents (ex. policy, terms of reference, toolkit) but specific oversight responsibilities, including frequency of reporting, could be more clearly defined.
	Medium	**5. Coordinated Risk Management and Assurance:** A framework, such as the Three Lines Model (Appendix D), could help increase collaboration across risk and assurance functions to improve efficiency and effectiveness of the overall Program.

Dimension	Risk	Key Findings
	Low	**6. Job Description:** The scope and major responsibilities are listed in the Corporate Risk Manager's job description, but it requires updating to reflect current reporting structure.
IT-Tools and Analyses	Medium	**7. Governance, Risk and Compliance (GRC) Tool:** The Program relies on manual Excel and Word tools. An integrated GRC tool would improve efficiency and effectiveness and facilitate continuous improvement. City Council has approved a capital project for a GRC tool.
Framework and Processes	High	**8. Risk Management Framework Implementation:** Detailed risk management toolkit and templates are available as are online training modules. However, there is no requirement to use them. Additional ELT support is needed to raise expectations and ensure broader use and implementation.

The above Findings and corresponding recommendations are intended to help improve the efficiency and effectiveness of the City's Risk Management Program. The report also includes items for future consideration (noted in *italics*) which could help continue the evolution and maturity of the Program but are not viewed as an immediate need.

Overall Administrative Response

The Administration agrees with all audit findings and is committed to the development of an ERM Strategy to assess, plan and roadmap the evolution of the City's ERM program and the implementation of the audit findings. The ERM Strategy and its associated roadmap will establish clear goals and timelines for the realization of measurable program outcomes. The evolution of the ERM program will leverage industry best practices and ensure this crucial capability meets the needs of the City. Planning will be dependent upon understanding the City's position and appetite relating to risk which is captured in Recommendation 1. The Administration is committed to the development of the strategy and roadmap by the end of Q4 2025. Target dates and timelines indicated within the individual Recommendations are at this point a best estimate and will be refined with the ERM planning and road mapping.

Next Steps

The Office is satisfied with the Administration's responses and will follow-up on their action plans to ensure they are appropriately implemented.
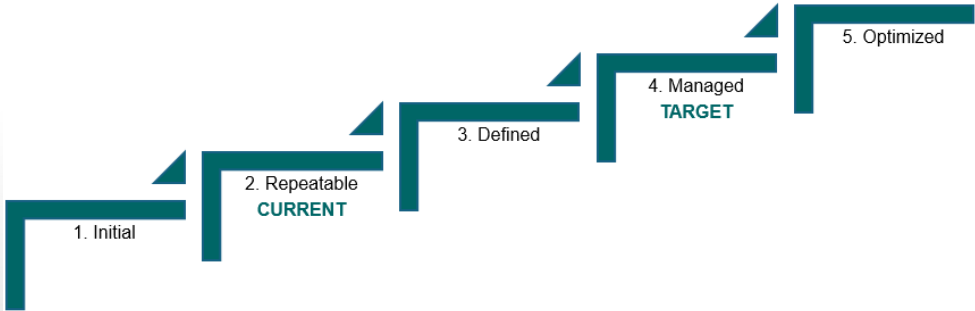
City of
Saskatoon

DETAILED REPORT

Risk Management, Strategy and Decision-Making Processes

This dimension evaluates the extent to which risk considerations are integrated into strategic planning, operational execution, and governance frameworks. It reflects how well the organization aligns its risk appetite with its strategic objectives, ensuring that decisions are informed by a balanced understanding of both opportunities and threats.

In a mature risk culture, risk management is not a compliance exercise nor a siloed function, but a strategic tool that supports proactive and value-driven decision making. Effective risk maturity in this area is characterized by proactive identification, assessment, and response to risks at all levels of decision-making. It requires leadership commitment, cross-functional collaboration, and the use of structured methodologies to ensure that risk insights shape strategic choices, resource allocation, and performance management. Organizations with high maturity leverage risk intelligence to navigate uncertainty and drive sustainable value creation.

The following table summarizes the maturity goal, criteria and assessment results for this 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.
Maturity Assessment Results	

Based on the maturity assessment for this dimension, the following two audit findings were identified.

Medium Risk	Risk Appetite
Finding #1	The Corporate Risk Appetite, which consists of fourteen individual risk appetite statements grouped into five risk categories, was approved by the Standing Policy Committee on Finance on March 5, 2018, but has not been subject to review since that date. Although noted in the March 5, 2018 Admin Report, the following planned activities have not been completed due to competing priorities and resource constraints: • Develop qualitative and/or quantitative metrics and risk tolerances to ensure the risk appetite is being embedded into the City's operations and risk-taking is aligned with the risk appetite. • Monitor actual performance in relation to those metrics and implement escalation procedures. • Update Council Policy No. C02-040, Corporate Governance – Risk Based Management Policy to include the Corporate Risk Appetite.
Recommendation #1	The Administration should: a. Review and update the Corporate Risk Appetite to ensure it is reflective of the current City Council's expectations. b. Define a regular review cycle to ensure the Corporate Risk Appetite stays current. c. Implement actions noted in the March 5, 2018 Admin Report (summarized in Finding above).
Administrative Response	*Response:* The Administration agrees with the recommendation. *Action Plan:* a. A high priority for the development of the ERM Program will be the update of the City's Corporate Risk Appetite by the end of Q2 2026. Going forward, this will be updated before (six months prior to) the strategic planning process every four years. Future Strategic plans will have a section within them for risk. b. A regular review cycle will be established for both City Council and for Administration by Q4 2025. c. The Risk Based Management Policy will be updated in accordance with the Corporate Risk roadmap in Q2 2026.

Medium Risk	Strategic Alignment, Integration and Documentation
Finding #2	Discussions with ELT members indicated that there is awareness of the Corporate Risk Appetite, but that it has not been formally integrated into decision-making processes, policy development and/or strategic planning. Further, the ELT indicated that although risk discussions are embedded into their regular meetings, the risk assessment process could be more formalized. The survey of Directors noted awareness of the Corporate Risk Appetite (79.4% Agree or Strongly Agree) and Risk Management Policy, Process and Toolkit (67.6%, 79.4% and 70.6%, respectively). However, the same survey indicated that only 29% of Directors regularly refer to and/or apply these Risk Management documents/tools.

City of
Saskatoon

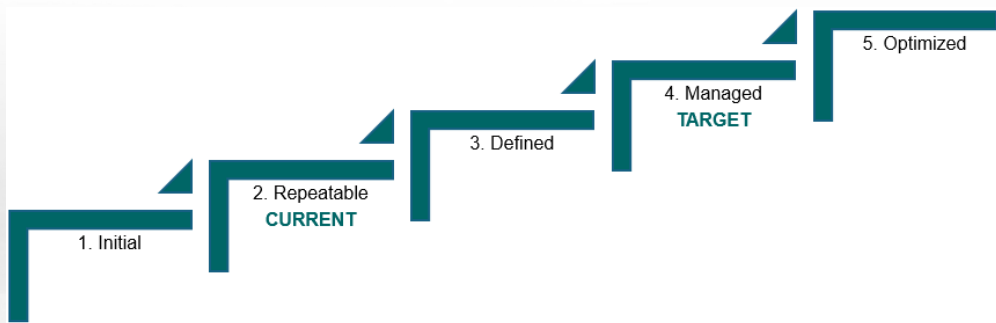| Medium Risk	Strategic Alignment, Integration and Documentation
	Integration of risk management into strategic planning and project management have been previously recommended as follows: • Infrastructure Investment Evaluation Process Audit recommended (#4) integrating risk within the strategic planning process. The Corporate Risk Manager has been involved in the 2026-2029 strategic planning sessions and, effective August 16, 2025, reports into the Business Transformation Department of the Strategy & Transformation Division (formerly reporting directly to the CFO). • Project Management Process Audit recommended (#1 and #7) updating the project management standard and framework and enhance consistent implementation (including project risk management). On June 26, 2025, the Administrative Leadership Team (ALT) approved resolutions stemming from the audit and actions are in progress. The status of the above previous recommendations will be followed up and reported separately.
Recommendation #2	The Administration should: a. Continue to support the integration and alignment of Risk Management and Strategy functions. b. Outline the expectations and create a standardized approach for recording risks and opportunities in decision-making processes. Risk assessments should be required for all major initiatives, policies, and capital projects (threshold to be defined). c. Incorporate Corporate Risk Appetite into future policy development and reviews, as appropriate. *Future Improvement Opportunity (no action plan required): The Administration should consider integrating risk into performance metric reporting.*
Administrative Response	*Response:* The Administration agrees with the recommendation. *Action Plan:* a. Concerted effort has recently been focused on more closely aligning Corporate Risk and Corporate Strategy activities and with the recent reorganization in the Strategy and Transformation Division, this partnership will be strengthened over the next several years as major corporate initiatives are undertaken (e.g., strategic planning, business planning, periodic status reporting, etc.). A specific plan to integrate ERM with Strategic Planning will be in place by Q2 2026. b. Continued ELT buy-in and involvement will be key to achieving widespread incorporation of risk into decision making and they will therefore be involved throughout 2026 in developing the expectations, adopting the approaches and determining the criteria for when risk evaluations are required. c. A plan to incorporate risk appetite into the Quality Management System (QMS) processes and future policy development will be developed in 2026.

City of Saskatoon

Medium Risk	Strategic Alignment, Integration and Documentation
	The operationalization and adoption of recommendations b and c will likely require significant Organizational Change Management planning (OCM) and will require ongoing work well into 2027 to fully realize.

Communication, Information and Reporting

This dimension evaluates the effectiveness of communication and information flow related to risk management within an organization. It focuses on the extent to which risk insights are consistently and transparently communicated across all levels, enabling informed decision-making and fostering accountability.

Structured communication plans, supported by governance mechanisms and quality assurance processes, are essential to ensure that risk-related data such as performance metrics, improvement actions, and emerging threats is timely, accurate, and accessible to relevant stakeholders. Mature organizations leverage dashboards and other formal channels to embed risk communication into their operational processes and strategic initiatives. By achieving high maturity in this dimension, organizations position risk management as a strategic enabler, ensuring that risk intelligence informs decisions, drives resilience, and supports sustainable value creation.

The following table summarizes the maturity goal, criteria and assessment results for this dimension.

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 are 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.
Maturity Assessment Results	

Based on the maturity assessment for this dimension, the following audit finding was identified.

High Risk	Risk Information and Reporting
Finding #3	Corporate Risk does not currently generate any stand-alone risk reporting and there is currently no overall risk reporting to enable oversight of risk management effectiveness. The Corporate Risk 2018 Annual Report represents the last time the City's strategic risks were assessed and reported. The ELT indicated that risk is considered as part of regular discussions. Also, risk information is reported in other means, such as: • Operating Budget includes "Key Risks and Mitigation Strategies" for each Business Line. Various budget reports include the identification of the "risk of not" (i.e., if not funded or without positions). • City Council and Committee reporting includes an "other implications" section which is intended to include risk considerations. Decision reports should include option analysis, including risks and opportunities for each. However, these are not specifically required, and reporting could vary. The Risk Management Toolkit provides a template and instructions for Departments to prepare Risk Registers. In addition, the Corporate Risk Manager had incorporated risk into project management templates and created Fraud Risk Assessments for each Division. The survey of Directors noted that 64.7% of departments have documented risk assessments. However, the Corporate Risk Manager is not always involved in the preparation or review process. The lack of a centralized risk repository limits transparency, results in risk information not being readily available for decision-makers and can hinder sharing of best practices/lessons learned. Most of the comparative organizations (Appendix B) have multiple levels of risk registers (ex. Strategic/Corporate and Division/Department) including regular updates and reporting.
Recommendation #3	The Administration should: a. Review and update the City's strategic risk register and present it to City Council. b. Implement a central repository of operational risks including project and fraud risks. (It may be more efficient to implement a central repository after an integrated Governance, Risk and Compliance (GRC) solution is in place, see Finding #7) c. Define and implement a regular review and reporting cycle to ensure strategic and operational risk registers remain current. The reporting process should include clear quality assurance measures to ensure consistency and reliability. (This should be considered as part of Finding #4) d. Define and implement a lesson learned process for significant risk events (threshold to be defined) to understand the causes of the risk event and facilitate continuous improvement of the risk mitigation activities and effectiveness of the Program.
Administrative Response	*Response:* The Administration agrees with the recommendation. *Action Plan:*

City of Saskatoon

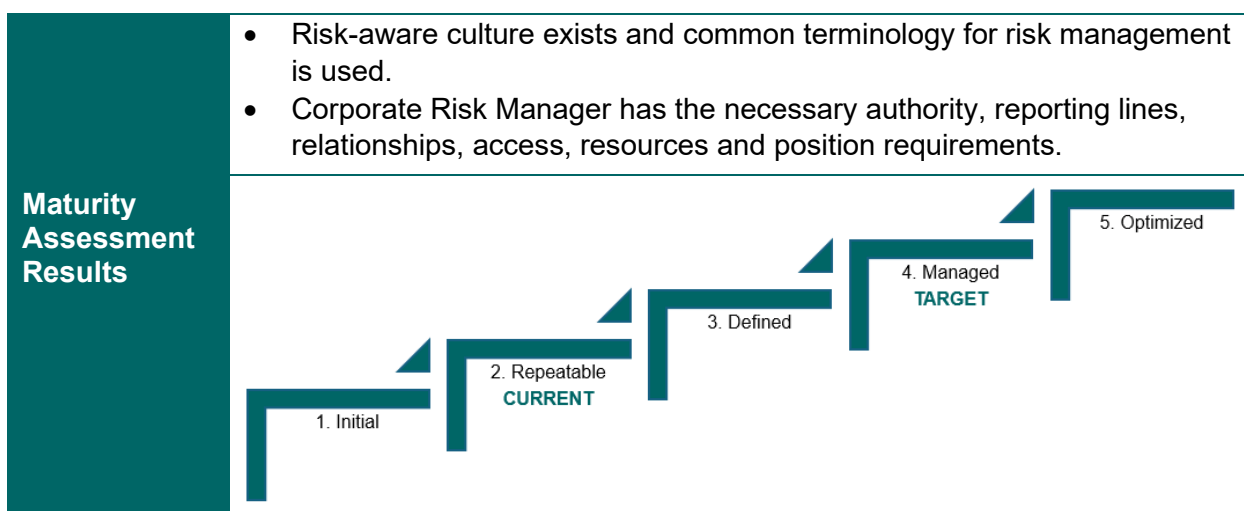| High Risk	Risk Information and Reporting
	a. A strategic risk assessment will be undertaken in Q1 2026 after the City's strategic plan is approved. The results of this assessment will be presented to City Council upon its completion. Going forward, these assessments will take place prior to the strategic planning process to provide input into the strategic planning decisions. b. The implementation of a repository and supporting platform are largely discussed in Finding #7. Work to develop needed processes, governance, and implementation plans can be done in parallel to the GRC platform planning. Initial planning work will commence in 2025. The implementation of the GRC solution, to support this capability, will need to be planned. This work is a high priority that will need to take place early in the ERM Program roadmap. Key features of the GRC solution will include the ability to efficiently review and update information with risk owners on a regular basis, generate reports and track verification procedures and results. c. The definition of regular reviews and reporting frequency to ensure strategic and operational risk registers remain current and include quality assurance measures to ensure consistency and reliability will likely be implemented in phases. Initial process planning and targets would likely take place in mid-2026. d. A lesson learned process will be developed and implemented within the GRC solution. Initial process planning work can potentially begin in mid-2026. Implementation would likely be late 2026 or early 2027.

Organization, Authority and Interaction

This dimension assesses how clearly defined roles, responsibilities, and lines of authority support effective risk governance and collaboration across the organization. It also evaluates the quality of interaction between key stakeholders such as executive leadership, risk management, and operational units ensuring that risk-related information flows freely and decisions are made with shared understanding.

A mature risk culture ensures that risk ownership is embedded at all levels, with accountability structures that empower individuals to act within their mandate while escalating issues appropriately to have enterprise-wide risk ownership. High maturity in this area reflects a well-aligned organization where collaboration fosters proactive risk management and informed decision-making.

The following table summarizes the maturity goal, criteria and assessment results for this dimension.

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 ELT.

City of **Saskatoon**

Maturity Assessment Results	• Risk-aware culture exists and common terminology for risk management is used.
	• Corporate Risk Manager has the necessary authority, reporting lines, relationships, access, resources and position requirements.

Based on the maturity assessment for this dimension, the following three audit findings were identified.

High Risk	Risk Management Oversight
Finding #4	Council Policy C02-040 Corporate Governance – Risk Based Management (RBM) Policy indicates that City Council "shall be responsible to set and review risk management policy" (section 4.1) but does not define ongoing risk management oversight responsibilities.
	The City Manager is "responsible for risk management throughout the corporation of the City" (RBM Policy, section 4.2), while the Administrative Leadership Team (ALT) is responsible to "identify and assess organizational risks and develop and implement risk mitigation strategies" (ALT Terms of Reference, section C.7). ELT members indicated that risk discussions are embedded into their regular meetings but acknowledged that the risk management process could be more formal.
	Most of the comparative organizations (Appendix B) have an oversight committee for the risk management function, including regular reporting.
Recommendation #4	The Administration should clearly define risk management oversight responsibilities, including frequency of reporting, at the City Council level as well as internally (through ALT and/or administrative standing committees) and update the relevant policies and/or terms of reference.
Administrative Response	*Response:* The Administration agrees with the recommendation.
	Action Plan: Governance and oversight responsibilities will be reviewed and incorporated into the Risk Based Management Policy and Standing Committee Terms of Reference in 2026 (timeline yet to be determined). Specific reporting obligations, frequency, target audiences, and content will be established by Q3 2026. The reporting frequency will be established during the ERM Program planning including a yearly update to City Council and a quarterly or bi-annual information report to the Administration's governance committees and ELT. Strategic risk

City of Saskatoon

High Risk	Risk Management Oversight
	reporting will accompany other strategic plan performance reports and updates to City Council in 2027.

Medium Risk	Coordinated Risk Management and Assurance
Finding #5	The Corporate Risk Management function has limited resources, operating as a one-person unit without access to an integrated Governance, Risk & Compliance (GRC) solution (Finding #7). Although similar staffing levels exist in government-related organizations (Appendix B), the reliance on manual and inefficient processes limits scalability and impact.

Due to the lack of centralized risk repository and regular risk reporting, it is difficult to determine whether ownership and accountability for each of the City's strategic and operational risks have been appropriately assigned, managed and monitored.

A structured governance framework, such as the Three Lines Model (Appendix D), could help clarify roles and responsibilities, improve collaboration across functions to improve efficiency and effectiveness of the overall Program. |
| Recommendation #5 | The Administration should consider adopting the Three Lines Model or similar governance framework, including developing a strategy for implementation. |
| Administrative Response | *Response:* The Administration agrees with the recommendation.

Action Plan: We have adopted the principles of the Three Lines Model and have started to incorporate them into the QMS. The development of the ERM Program strategy will also include the identification of best practices and governance framework(s) to be used. This work will commence before the end of 2025, and a timeline and roadmap will be developed to improve maturity in this area. The realization of the desired outcomes will require sound adoption planning, including Change Management to be successful. An updated timeline will be produced once initial planning completes early in 2026. |
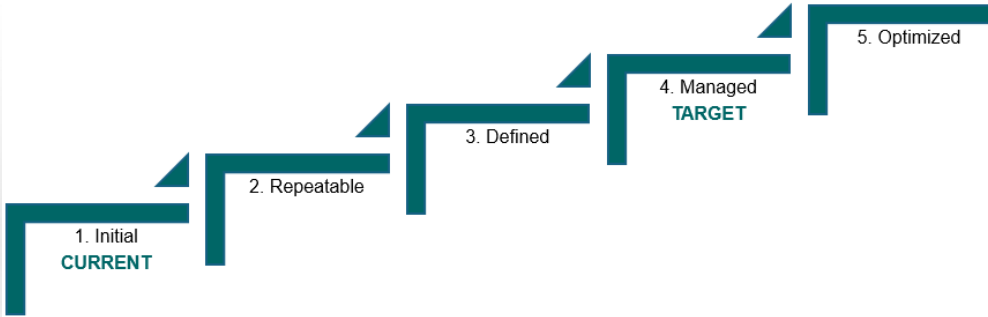
Low Risk	Job Description
Finding #6	The scope and major responsibilities listed in the Corporate Risk Manager's job description are generally consistent with the activities of a mature risk management function. However, it still refers to managing the outsourced internal audit function, which was in place from 2015 to 2019, and should be refreshed as part of the recent reorganization.

As noted in Finding #2, the Corporate Risk Manager's reporting relationship recently changed from the CFO to the Director, Business Transformation. Comparison with other organizations (Appendix B) |

Low Risk	Job Description
	revealed that there is no "one size fits all" approach to structuring a risk management function in terms of title, functional area or reporting relationship.
Recommendation #6	The Administration should review and update the Job Description for the Corporate Risk Manager.
Administrative Response	*Response:* The Administration agrees with the recommendation.
	Action Plan: The Corporate Risk Manager's job description will be updated to reflect current responsibilities and reporting structure prior to year end 2025.

IT-tools and Analyses

This dimension assesses how effectively an organization uses digital tools and data analytics to support risk management. At lower maturity levels, risk processes may rely on manual tracking and basic software. As maturity increases, an organization adopts integrated systems and data-driven tools that enhance risk identification, analysis, and decision-making, enabling more proactive and transparent governance. Use of technology enhances risk visibility and monitoring, data-driven decision making, improved efficiency, consistency, and better integration of risk management across functions.

The following table summarizes the maturity goal, criteria and assessment results for this dimension.

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 the 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.
Maturity Assessment Results	

Maturity levels shown in diagram: 1. Initial **CURRENT**, 2. Repeatable, 3. Defined, 4. Managed **TARGET**, 5. Optimized

Based on the maturity assessment for this dimension, the following audit finding was identified.
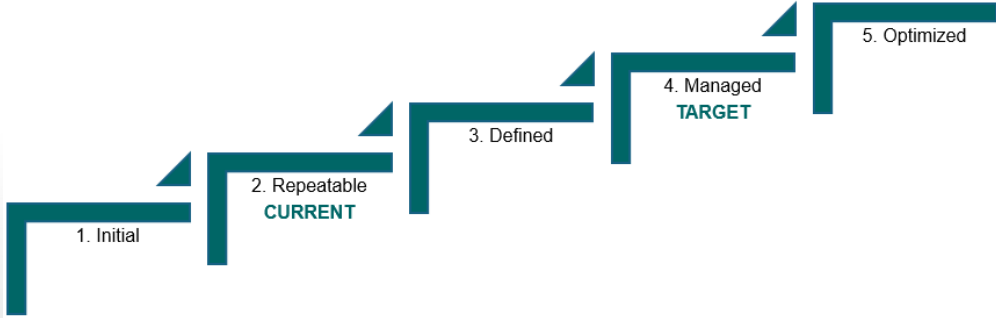
Medium Risk	Governance, Risk and Compliance (GRC) Tool
Finding #7	The City's Corporate Risk Management Program relies on Microsoft Office tools (i.e., Excel and Word) which are manual in nature and may be applied inconsistently. Although this is a common approach when comparing it with other organizations (Appendix B), it is not the most effective and efficient. It can also lead to siloed efforts and does not facilitate sharing of best practices and continuous improvement.

The City Auditor and the Corporate Risk Manager have discussed the use of an integrated Governance, Risk and Compliance (GRC) tool that would benefit both functions. Implementation of a GRC tool could enable further maturity of the Risk Management Program including dashboard reporting, data-informed risk analysis and ongoing risk monitoring. On May 21, 2025, City Council approved a capital project for an integrated GRC solution to be funded by the Internal Audit Program Reserve. |
| Recommendation #7 | The Administration, in partnership with the City Auditor should implement an integrated GRC solution. The Administration should be responsible for:

a. Implementing the appropriate risk management processes within the relevant GRC module.
b. Coordinating the development of a central repository of the City's strategic and operational risks, including assignment of individual risk owners and identification of risk mitigation activities.
c. Ensuring appropriate access and risk management training is provided to applicable users.

Future Improvement Opportunity (no action plan required): The Administration should consider implementing dashboard reporting, data-informed risk analysis and ongoing risk monitoring once the GRC solution is implemented and stabilized. |
| Administrative Response | *Response:* The Administration agrees with the recommendation.

Action Plan:

a. As part of the ERM strategic plan, the Corporate Risk Manager will work with the City Auditor, the City's Enterprise Architect, and Digital Technology to identify, procure, and implement a GRC solution. Initial exploratory conversations have been taking place, and we hope to put a plan in motion before the end of 2025.
b. By design and as part of this implementation, it will ensure that risk management responsibilities are properly assumed in order to maintain the independence of the City Auditor's Office. Once the platform and processes are in place, there will be significant effort in holistically populating the central repository. Timelines for this will be established at a later point in the ERM roadmap.
c. As part of this initiative, a risk management training plan will be developed to ensure the training needed is available for the applicable users. This will evolve in stages, some of which will be started in Q2 2026 and will continue to evolve as this aspect of the program is realized. |

Framework and Process

This dimension evaluates the structure, clarity, and integration of the risk management framework and processes. It considers whether risk management is embedded in strategic and operational planning, supported by clear roles, responsibilities, and procedures. A mature organization will have a well-documented, consistently applied framework that guides risk identification, assessment, response, and ongoing evaluation/monitoring across all departments, enabling informed decision-making and accountability.

Best practices in this area include aligning the risk framework with organizational objectives, ensuring that it is scalable and adaptable to changing contexts. The framework should be supported by standardized tools and templates, periodic reviews, and integration with performance management and governance structures. Organizations demonstrating high maturity in this dimension use their framework not only to manage risks but to anticipate them, thereby turning risk management into a strategic capability that drives resilience, innovation, and long-term value creation.

The following table summarizes the maturity goal, criteria and assessment results for this dimension.

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.
Maturity Assessment Results	

Based on the maturity assessment for this dimension, the following audit finding was identified.

High Risk	Risk Management Framework Implementation
Finding #8	The Program is based on the methodology outlined in ISO 31000 Risk management – Guidelines (Appendix A) which is consistent with almost all of the comparative organizations (Appendix B).

High Risk	Risk Management Framework Implementation
	The purpose and mandate of the Program is defined in Council Policy C02-040 Corporate Governance – Risk Based Management (RBM) Policy. The Policy indicates that all City employees are "responsible for management of risk and uncertainty within the scope of their duties and shall comply with requirements of the RBM system" (section 4.4). However, the Corporate Risk Manager does not have the authority to ensure compliance with the Policy and lacks the influence and resources required to ensure the effectiveness of the Program. Although the Corporate Risk Manager has developed common risk terminology, tools, templates (including for general use as well as project and fraud specific) and processes, and based on the survey of Directors has built strong relationships and received positive feedback, these strengths are not yet supported by formal systems or sustained practices. For example: • The Policy is supported by a detailed Risk Management Toolkit and Templates, but their implementation and usage is optional. • Risk management training modules are available through the Supervisor 101 Program in SuccessFactors, but they are not mandatory. Conversely, fraud risk awareness is embedded into the performance evaluation signoff process and training is mandatory for all new employees as of January 2025. Although the survey of Directors indicates that risks are well managed, it is not necessarily in a consistent, repeatable and documented manner. Of note, the survey indicates that (% agree or strongly agree): • Decisions are made within the approved risk appetite (74%) • Risk management is embedded into daily operations (67%) • The City actively promotes a risk-aware culture (59%) • Employees have adequate risk management training (35%) • Directors regularly refer to and/or apply the City's Risk Management policy, process, toolkit and/or appetite (29%)
Recommendation #8	The Administration should: a. Elevate, support and promote the Risk Management function and encourage its full adoption across the City. b. Ensure compliance of section 4.4 of the RBM Policy within their respective Divisions. This could help ensure more consistent and formal implementation of the Risk Management Process. c. Consider making the current Risk Management training modules mandatory for certain employee levels. This could help create further awareness and appreciation of the purpose and benefit of the risk management processes.
Administrative Response	*Response:* The Administration agrees with the recommendation. *Action Plan:* a. As part of the ERM Strategic Plan, a communication, adoption, and promotion plan will be developed to ensure the incorporation of ERM practices across the City by the end of Q2 2026.

High Risk	Risk Management Framework Implementation
	b. This ERM strategic plan will assess the requirements of section 4.4 of the RBM Policy and establish a path forward and address compliance where needed. c. An ERM Program training plan will be developed that will verify the needed curriculum and determine if or what training should be mandatory. It is likely that this curriculum will evolve over time as specifics regarding supporting implementation, operationalization, and OCM challenges and impacts are better understood. Initial planning would likely commence by Q2 2026.

APPENDICES

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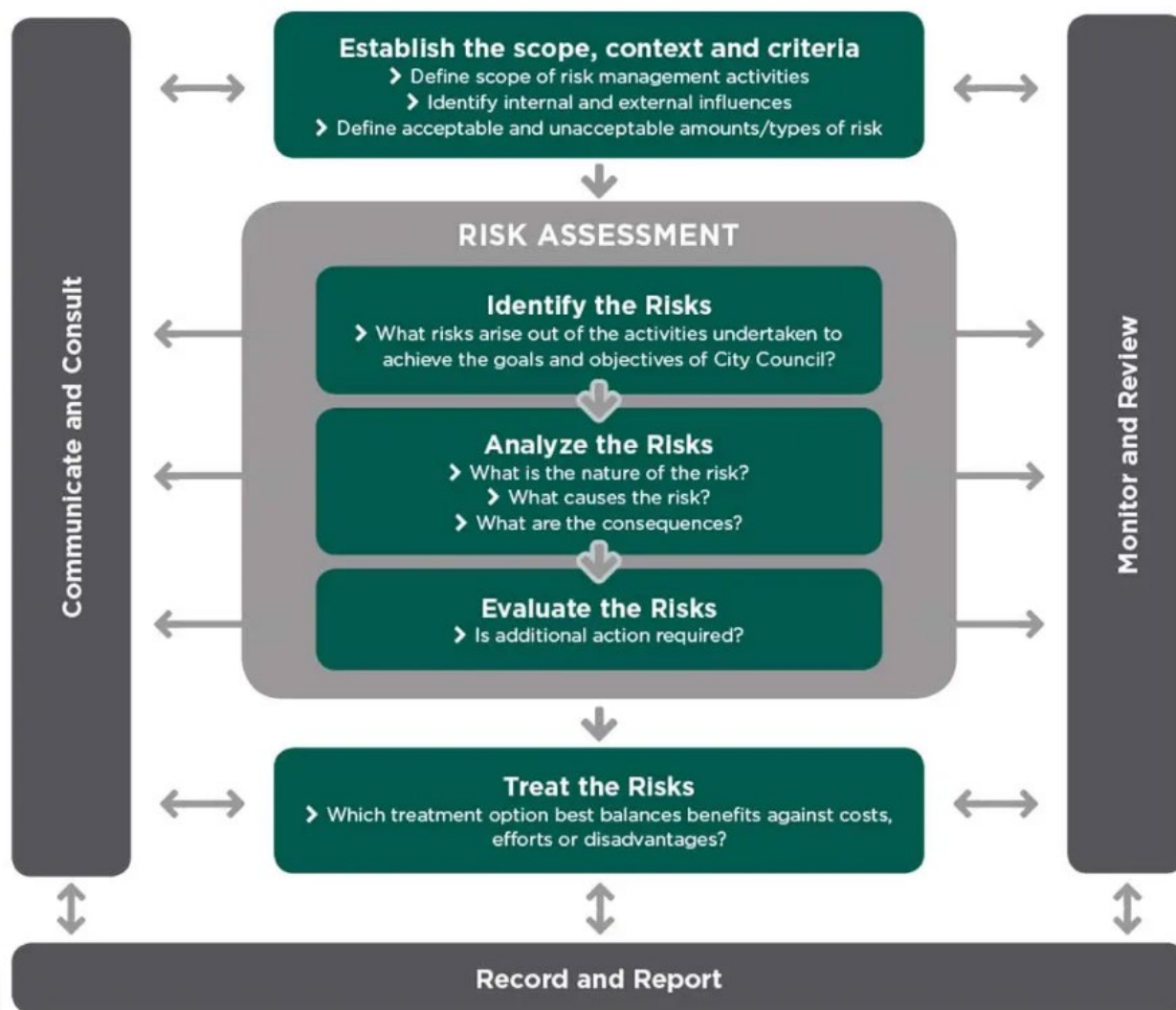
Source: Corporate Risk 2018 Annual Report (page 6)
https://www.saskatoon.ca/sites/default/files/documents/corporaterisk-2018ar_-_web_version.pdf, adapted from ISO 31000:2018 Risk management – Guidelines.

Appendix B – Comparison to Other Organizations

The Office contacted several Canadian municipalities and provincial government-related organizations to request information about their respective risk management programs. Information was received from three cities (identified as C1 to C3) and four government-related organizations (identified as O1 to O4) under the agreement that their information would be anonymized for reporting purposes.

The table below provides a summary of the comparison of Saskatoon and these seven participating organizations. Note that this information has not been subject to audit or verification by the Office and is based on responses received and is presented for informational purposes only.

Factor	Saskatoon	C1	C2	C3	O1	O2	O3	O4
Population (2024)	~300,000	>1,000,000	>1,000,000	>1,000,000	n/a	n/a	n/a	n/a
Risk Function Head (title)	Manager	Director	Director/ CRO	Manager	Director	Director	Director	Coordinator
FTE	1	No dedicated	7	3	No dedicated	1.5	1	0.5
Functional Area	Strategy & Transformation	Strategy	Finance	City Manager's Admin Branch	Internal Audit	Internal Audit	Finance	ERM
Risk Function Reports to	Director	ELT	CFO	City Manager's Office	Board Committee / President	Executive VP Legal	CFO	Board Committee
Internal Risk Committee	Yes (ALT)	Yes	No (in progress)	No (reports to Council)	Yes (Executive)	Yes (Executive)	Yes (Executive)	Yes (Executive)
Policy & Framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Methodology Based on	ISO	ISO	ISO	ISO	COSO	ISO	ISO	ISO
Risk Register (levels)	Strategic / Fraud	Strategic / Department / Branch	Corporate / Service	Central / Dept.	Corporate / Department	Corporate / Division	Corporate / Division	Central
Risk Register Updates	n/a	Annual	Semi-annual	Annual	Quarterly & Annual	Annual	Quarterly	Annual
Reporting Frequency	None	Annual	Semi-annual	Twice per Council term	Quarterly	Continuous	Quarterly	Continuous
Tools	Spreadsheets / Word	Spreadsheets	SharePoint / Spreadsheets	Spreadsheets	Spreadsheet / Power BI	TeamMate+ / Spreadsheets	Word / PowerPoint	Spreadsheets / Word

Abbreviations:
- CRO – Chief Risk Officer
- ISO – International Organization for Standardization 31000:2018 Risk management – Guidelines
- COSO – Committee of Sponsoring Organizations Enterprise Risk Management – Integrating with Strategy and Performance (ERM Framework)

Appendix C – Risk Rating Guide

The Independent Office of the City Auditor has introduced a risk rating to prioritize the audit recommendations in the report. The benefits of the rating are to:

- Help Administration and City Council to assess results quickly.
- Help Administration to prioritize implementation of the recommendations.
- Provides the basis for prioritizing audit follow-up.
- Makes cross-organizational comparison easier.

Criteria	Risk Rating
Corporate level loss, material reporting misstatement, critical reputation, or financial impact; critical impact on operational performance, the occurrence of fraudulent activities, critical unethical conduct, or a critical breach in laws and regulations/policies and procedures. Remediation of the finding should be immediately prioritized.	**Critical**
Significant impact on the achievement of objectives. Significant risk of service disruption, a threat to timely and effective service delivery affecting clients or a high possibility of occurrence of fraud. High-risk impact on reputation, financial, or operations. A significant breach in laws and regulations and policies and procedures.	**High**
Moderate impact on the achievement of objectives. Moderate risk of service disruptions, a threat to timely and effective service delivery affecting clients or occurrence of fraud. Moderate risk impact on reputation, financial, or operations. A moderate breach in laws and regulations/policies and procedures. Requiring process change/improvement to reduce the likelihood or impact of the risk in the future.	**Medium**
Minor impact to the achievement of objectives. Low/minimal risk of service disruption, threat to timely and effective service delivery affecting clients. Low risk impact on reputation, financial, or operations or occurrence of fraud. Minor breach in laws and regulations / policies and procedures with limited consequences. Value added process improvement or enhancement.	**Low**

City of Saskatoon

Appendix D – The IIA's Three Lines Model
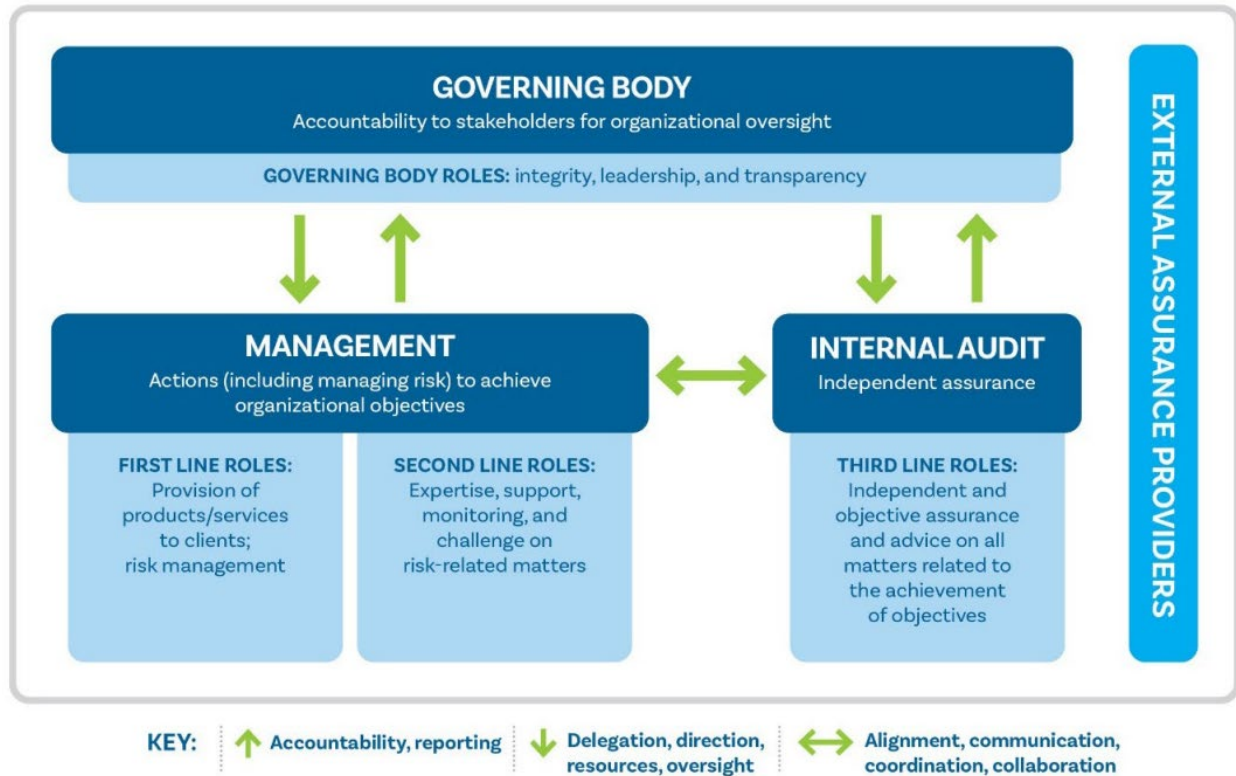
Source: The IIA's Three Lines Model: An update of the Three Lines of Defense (2020, updated 2024). ©2024, The Institute of Internal Auditors, Inc. Used by permission; available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf