OFFICE OF
THE CITY AUDITOR

REPORT

ENTERPRISE RISK MANAGEMENT PROGRAM AUDIT

AUGUST 14, 2025

Report Summary

BACKGROUND

Enterprise Risk Management (ERM) provides the City with a framework for identifying, assessing, and mitigating risks. ERM allows organizations to make decisions that are based on a comprehensive understanding of potential threats and opportunities.

By integrating risk considerations into its strategic planning and daily operations, the City can make better-informed decisions, strengthen its organizational resilience, and support the achievement of its strategic objectives.

AUDIT OBJECTIVE & SCOPE[1]

The objective of this audit was to determine the maturity of the City's enterprise risk management program against best practices.

The scope of this audit included all areas of the City under the authority of the City Manager and City Auditor. The audit was conducted from April to July, 2025. This audit did not review the management of individual risks.

USE OF A SUBJECT MATTER EXPERT

The Office of the City Auditor plays a role in the City's enterprise risk management. To avoid potential biases in this audit, we engaged an external subject matter expert to conduct a maturity assessment. The findings and conclusions included in this report are based on the subject matter expert's findings.

MATURITY ASSESSMENT SCALE

This audit assessed how effectively the City has implemented the five interrelated components of enterprise risk management into the City's ERM approach:

1. Governance & Culture
2. Strategy & Objective-Setting

[1] We (the Office of the City Auditor) conducted this engagement in conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

3. Performance
4. Review & Revision
5. Information, Communication & Reporting

For this audit, we used a five-stage maturity model to describe the City's capabilities for each component of enterprise risk management. See Figure 4 (page 12) for descriptions of the following five phases of maturity in an ERM program:

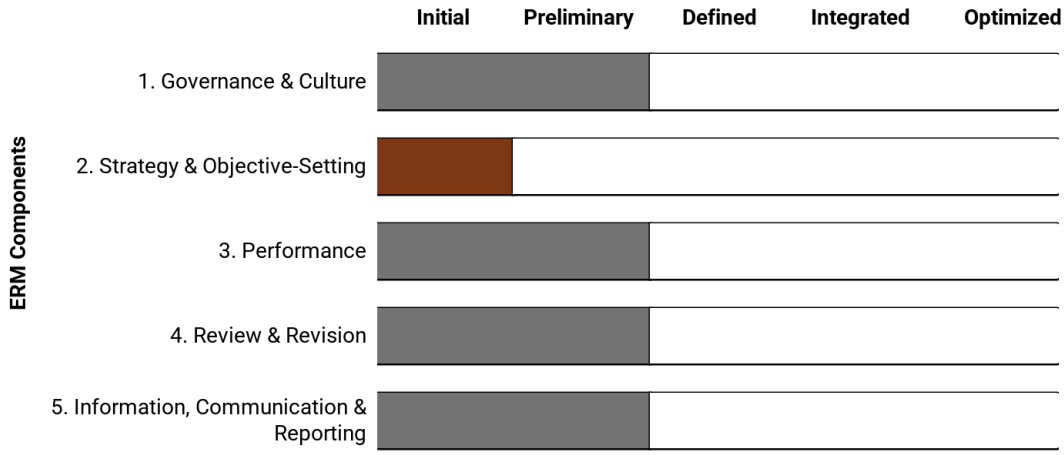
1. Initial
2. Preliminary
3. Defined
4. Integrated
5. Optimized

WHAT WE FOUND[2] - MATURITY ASSESSMENT RESULTS

Overall, we found that the City has made strides to advance the integration of its ERM program into its governance, operations and planning functions. For example, the City has some good foundational ERM processes and procedures in place. However, the City's approach lacks necessary components of a mature program as well as consistency of ERM practices across functions and leadership levels. This is reflected in the maturity assessment for each of the core components. (Figure 1)

[2] The Institute of Internal Auditors' *Global Internal Audit Standards* require us to report the significance and prioritization of our findings. This report contains all our significant findings and those that we deemed not significant, but that still support our recommendations. We prioritized each significant finding based on how important it is that management address the finding. This report contains only those significant findings that we prioritized as management must address, or should address.

Figure 1: City of Edmonton Enterprise Risk Management Maturity Scorecard



Governance & Culture

We assessed the City to be in the Preliminary Phase for Governance & Culture.

Senior management has demonstrated a strong understanding of The City Plan[3] and its relationship with ERM. In addition, the City has an ERM program in place, which includes an ERM policy and a Risk Committee tasked with supporting the City's ERM program. However, we found that there is a disconnect between stated priorities, guiding documents, and practical implementation.

To enhance the City's maturity within this component, it will need to:

- Enhance its governance over ERM to include:
  - Updated documentation on the owner of the City's enterprise risk management program.
  - A formal process to evaluate and track ERM maturity, lessons learned, and refinements across the system.

[3] Edmonton's City Plan, Charter Bylaw 20000, set strategic direction for the way Edmonton grows, its mobility systems, open spaces, employment and social networks.

    - A communication strategy to ensure all staff levels receive timely and appropriate risk and performance information.
- Enhance ERM education, including but not limited to training, supporting documentation, and communication of roles and responsibilities.
- Dedicate resources towards implementing the ERM program and supporting the Risk Committee.

Strategy & Objective-Setting

We assessed the City to be in the Initial Phase for Strategy & Objective-Setting.

We found that Council involvement in approving business plans ensures that strategic goals are aligned with public policy mandates and that risk is a factor in major decisions.

However, we also found a misalignment between the City's ERM program, strategy, and objective-setting processes. This is primarily due to the absence of defined risk appetite statements, which means that it is unclear how much risk the City is willing to accept in the pursuit of its objectives.

To enhance the City's maturity within this component, it will need to:

- Define its risk appetite and tolerance thresholds for each of its defined risk categories, for example financial risk and environment risk.
- Implement consistent, city-wide methodologies for identifying, assessing, prioritizing, and responding to risks within those thresholds.

Performance

We assessed the City to be in the Preliminary Phase for Performance.

We found that the Executive Leadership Team (ELT) and branch managers use performance reporting tools such as dashboards and performance measures to track progress against business or service plans.

However, we also found that these performance reviews are often conducted in isolation from strategy, objective-setting, and risk management processes, limiting feedback loops between outcomes, strategy and objectives, and risk posture[4]. In addition, we found that ERM-related activities lack uniformity across the organization.

To enhance the City's maturity within this component, it will need to implement consistent, city-wide methodologies for identifying, assessing, prioritizing, and responding to risks within the risk appetite and tolerance thresholds.

Review & Revision

We assessed the City to be in the Preliminary Phase for Review & Revision.

We found that senior leadership review risk registers[5] on a quarterly and annual basis, and use them to evaluate the City's overall risk portfolio. The Risk Committee provides structured oversight through annual reviews of corporate risk documentation. However, ERM should not be a static exercise. It should be a dynamic system that evolves with the organization and its environment, driving continuous improvement and strategic resilience.

We also found the City has an ad hoc, informal process for identifying and assessing internal and external changes that substantially impact strategy or objectives.

To enhance the City's maturity within this component, it will need to develop and communicate an integrated process to evaluate and track ERM maturity and lessons learned, and then implement refinements across the system.

Information, Communication &

We assessed the City to be in the Preliminary Phase for Information, Communication & Reporting.

[4] Risk posture refers to an organization's overall risk exposure, considering its current controls and how effectively it manages those risks.

[5] Risk registers are documents that describe potential risks that could affect an area, along with their likelihood, impact, and approach to the risk.

Reporting

To fulfill their responsibilities, each employee needs to be aware of different kinds of detail and levels of risk related to their job performance. We found that the City's information and technology systems to support ERM are underdeveloped and inconsistently applied across the City. In addition, the City lacks an effective communication strategy to ensure relevant and risk information reaches the right people at the right time.

To enhance the City's maturity within this component, it will need to improve its ERM technology infrastructure as well as implement an effective communication strategy to ensure all staff levels receive timely and appropriate risk and performance information.

Our recommendations are intended to enhance the City's maturity within each component and grow the City's ERM program.

RECOMMENDATIONS

Recommendation 1

We recommend the Financial and Corporate Services Department enhance the Enterprise Risk Management Program to include:

- Updated documentation on the owner of the City's enterprise risk management program.
- A process to evaluate and track ERM maturity and lessons learned, and to implement refinements across the system.
- A communication strategy to ensure all staff levels receive timely and appropriate risk and performance information.

Recommendation 2

We recommend the Financial and Corporate Services Department, as part of the City's Enterprise Risk Management Program, develop and implement ERM education that ensures employees are aware of their roles and responsibilities in ERM,

including expectations to build a more broadly risk-aware culture and enhance ERM capabilities.

Recommendation 3

We recommend the Financial and Corporate Services Department dedicate resources towards increasing the level of ERM experience in the City, to assist in managing the ERM system and support the Risk Committee.

Recommendation 4

We recommend the Financial and Corporate Services Department, as part of the City's Enterprise Risk Management Program, define the City's risk appetite and tolerance thresholds for each risk category.

Recommendation 5

We recommend the Financial and Corporate Services Department develop consistent, city-wide methodologies for identifying, assessing, prioritizing, and responding to risks to formalize and integrate ERM practices. This includes applying risk appetite thresholds, ensuring real-time updates to risk registers, and linking ERM directly to business planning and corporate performance management and reporting.

Recommendation 6

We recommend the City Manager improve ERM's technology infrastructure to support centralized risk documentation and reporting.

WHY THIS IS IMPORTANT

Enhancing the City's ERM program by and integrating risk management into all levels of the organization will strengthen the City's culture of risk awareness, encouraging employees and management to proactively identify and mitigate risk. This will help the City become more resilient to unexpected events and disruptions, promote business continuity, and support the achievement of the City's strategic objectives.

City of Edmonton Enterprise Risk Management Program Details

BACKGROUND

Enterprise Risk Management (ERM) is the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.[6]

An ERM program provides a structured approach for identifying, assessing, and mitigating risks. This approach allows organizations to make informed decisions based on a comprehensive understanding of potential threats and opportunities.

The City's statement for the purpose of risk management is[7]:

> "We identify and anticipate the risks to the City in order to support effective decision making, strengthen resilience, and create opportunities to innovate the way we deliver services to Edmontonians."

The City of Edmonton's ERM program is governed by Council Policy C587A approved by City Council on December 12, 2023. Policy C587A is supported by the City's ERM Procedure.

THREE LINES MODEL

ERM is the overarching approach to managing all risks an organization faces. The three-lines model provides a practical approach to:

- Helping organizations implement ERM.
- Ensuring that all parts of the organization are

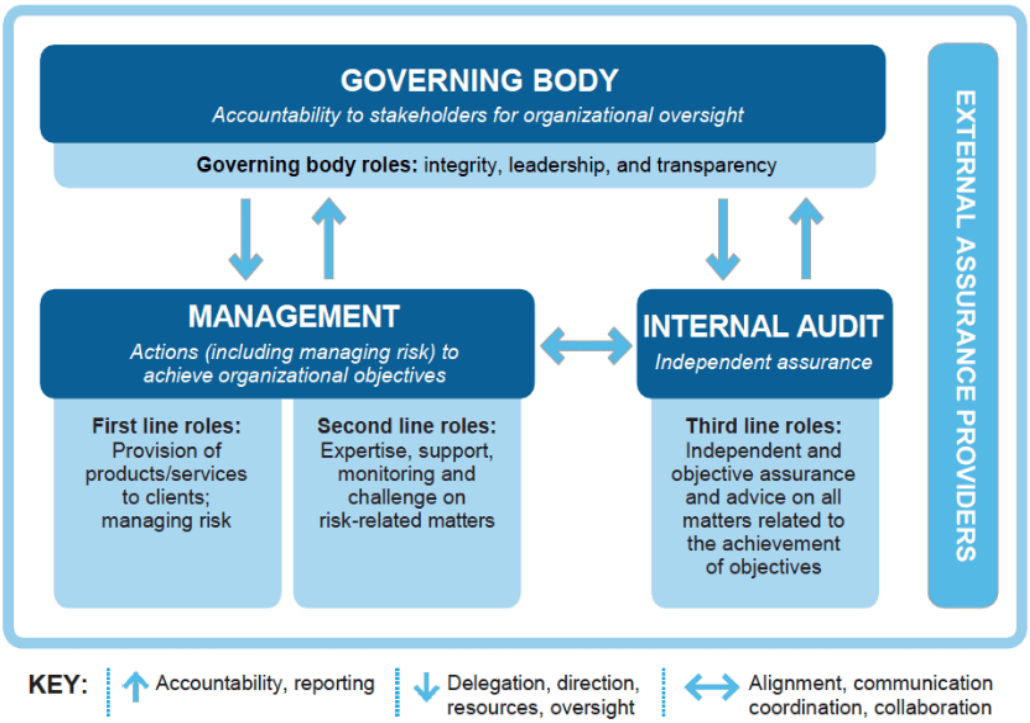
[6] COSO, *Enterprise Risk Management: Integrating Strategy and Performance* (2017)

[7] City of Edmonton, Finance and Corporate Services, *Enterprise Risk Management (ERM) Framework* (August 2023)

involved in managing risk.
- Establishing a robust system of oversight and assurance.

The model is based on the idea that an organization needs three lines of defense that work together to provide structure around risk management and internal governance (Figure 2).

Figure 2: Three Lines Model[8]



This project was undertaken as part of the Office of the City Auditor's responsibility as the third line of defense. Any actions resulting from this audit will be undertaken as part of management's first and second line roles.

ENTERPRISE RISK MANAGEMENT BEST PRACTICE

We used the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework (COSO Framework) as best practice for this audit. The COSO Framework consists of five interrelated

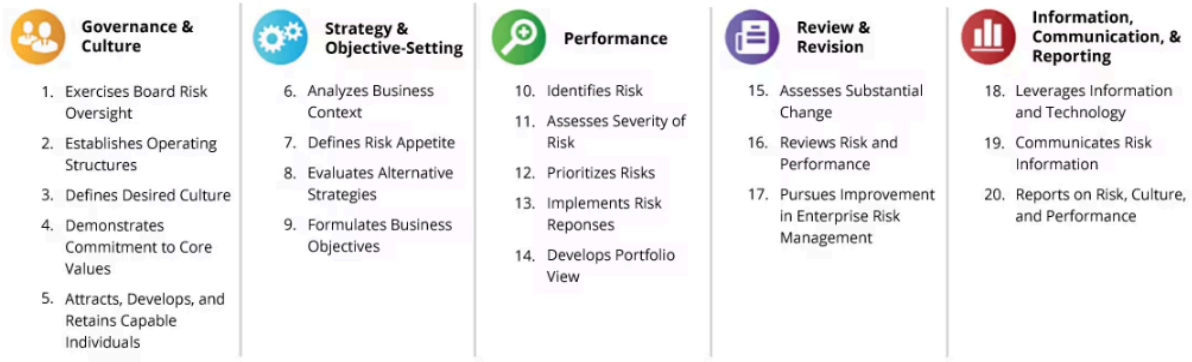
[8] Institute of Internal Auditors, *The IIA's Three Lines Model, An Update of the Three Lines of Defense (2024)*

components:

1. Governance & Culture
2. Strategy & Objective-Setting
3. Performance
4. Review & Revision
5. Information, Communication & Reporting

Each of the five components in the COSO Framework is supported by a set of principles (Figure 3). Adhering to these principles can provide City Council and Senior Management with a reasonable expectation that all employees understand and strive to manage the risks associated with the City's strategy and business objectives.

Figure 3: COSO Enterprise Risk Management Components and Principles[9]



For this audit, we considered how the City applies these ERM principles in the context of each component. In the following sections of this report, we provide:

- A brief description of each component and its principles.
- Our key findings to enhance the City's maturity within each component.
- Our recommendations to address the findings.

[9] COSO, *Enterprise Risk Management: Integrating Strategy and Performance* (2017)

MATURITY ASSESSMENT SCALE

We used the maturity scale shown in Figure 4 to describe the City's capabilities for each of the components of an ERM program. See Appendix A for the detailed ERM Maturity Model applied across the five components.

Figure 4: Enterprise Risk Management Maturity Scale

Initial	Preliminary	Defined	Integrated	Optimized
Processes are informal, undocumented, or inconsistent	Some processes exist but are inconsistently applied or not well understood.	Processes are documented and applied, though integration and consistency are limited.	Practices are embedded, consistently executed, and supported by tools and metrics.	Practices are strategic, proactive, optimized, and benchmarked against best-in-class organizations.

Component 1: Governance & Culture - Preliminary Phase

COMPONENT AND PRINCIPLES

The Governance & Culture component focuses on establishing the foundation for effective risk management throughout an organization. It emphasizes the importance of leadership, ethical values, and a strong organizational structure in creating a culture that supports risk awareness and mitigation.

This component sets the organization's tone by reinforcing the importance of ERM and establishing oversight responsibilities for ERM. It also defines desired behaviors and ethical values that guide the organization's understanding of risk.

Principles within the Governance & Culture component:

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Appendix B lists a detailed description of each of the principles.

KEY FINDINGS

We assessed the City to be in the Preliminary Phase for Governance & Culture.

Executive Leadership Team (ELT) members and branch managers expressed a strong understanding of The City Plan and its relationship with the ERM.

The City has an ERM policy and has formalized risk roles and responsibilities at the senior leadership level, including defined reporting lines to the Risk Committee and ELT.

In addition, the City has established a broad base of participation in ERM governance, with subject matter experts

and City-wide representation on the Risk Committee. Staff at the branch level also reported that risk discussions are embedded into their operational planning processes, indicating cultural uptake beyond executive ranks.

However, there is a lack of clarity around who is the owner of the City's ERM program. This means it is not understood who is accountable for the leadership for the ERM program and related processes.

In addition, we found that:

- There is no consistent approach to communicating risk culture expectations across the City. Many directors and front-line staff are uncertain about their roles with the ERM system.
- While leadership and senior management affirm risk culture as a priority, operational staff indicated that cultural expectations around risk are not embedded into daily workflows or performance expectations.
- There is a lack of formal mechanisms to reinforce ERM behaviors or expectations beyond high-level strategy documents.

Interviews with members of the Risk Committee indicated a need for more ERM expertise to support the work of the Risk Committee.

LACK OF CLARITY AROUND ERM OWNERSHIP

We found there is a lack of clarity around who is the owner of the City's ERM program. The City's ERM procedure states that "*the City Manager will foster a culture and philosophy of risk management through delegating authority and resources for Enterprise Risk Management*". The City Manager delegated this to the Deputy City Manager of the Financial and Corporate Services Department. However, the ERM Framework does not mention the Deputy City Manager of Financial and Corporate Services in its accountabilities. Further, the City's Risk Committee, which consists of internal subject matter experts specializing in risk management from across the organization,

does not have the Deputy City Manager of Financial and Corporate Services as its executive sponsor.

Additionally, we surveyed the City's branch managers and directors, with 61 people responding. We asked respondents who they thought is primarily responsible for the City's ERM program. Responses were widespread, with only 37.7% (23 out of 61) indicating that the Deputy City Manager of Financial and Corporate Services is primarily responsible for the City's ERM program. This indicates a lack of clarity around ownership of the City's ERM program. The following comment from one survey participant describes this problem well:

> *"The corporate organizational structure with multiple Deputy City Managers with multiple accountability touch points does not allow for adequate Enterprise Risk Management at an executive control level." - Survey Comment*

LACK OF CLARITY AROUND RISK CULTURE

We found several opportunities for improvement in the City's risk culture. Specifically, we observed a lack of consistency in how expectations regarding risk culture are communicated throughout the organization. This inconsistency may lead to uncertainty among directors and front-line staff about their roles and responsibilities within the ERM program.

Of the City branch managers and directors that we surveyed, 29.5 percent (18 of 61) either disagreed or were unsure if roles and responsibilities are clear when it comes to ERM in their department or branch (Chart 1). In addition, when asked about how well-defined the roles and responsibilities related to ERM are within the City, 41.0 percent (25 of 61) responded that they were unsure and 14.8 percent (9 of 61) responded that they were not well defined or not defined at all (Chart 2). Branch managers were more clear about ERM roles and responsibilities than directors.

Chart 1: Survey Results - Clarity of Branch or Section-Specific Risk Management Roles and Responsibilities

Survey Question:
Are roles and responsibilities clear when it comes to risk management within your branch or section?

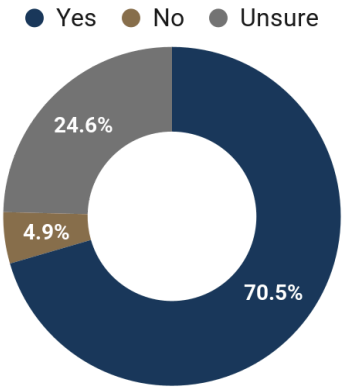
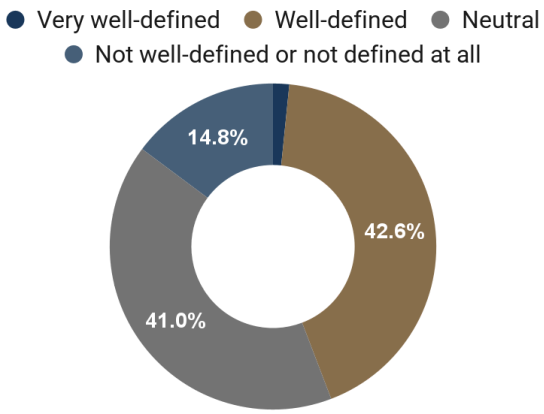


Chart 2: Survey Results - Definition of City-Wide ERM Roles and Responsibilities

Survey Question:
How well-defined are the roles and responsibilities related to ERM within the City?



Furthermore, despite leadership's verbal affirmation of risk culture as a priority, some directors reported that these cultural expectations are not effectively integrated into their daily workflows or performance metrics. Only about one third of survey respondents indicated that they or their team have received any training on risk assessment, risk management, or ERM principles and practices (Chart 3 and Chart 4).

Chart 3: Survey Results - Risk Assessment and Risk Management Training

Survey Question:
Have you and your team received any risk assessment and risk management training?

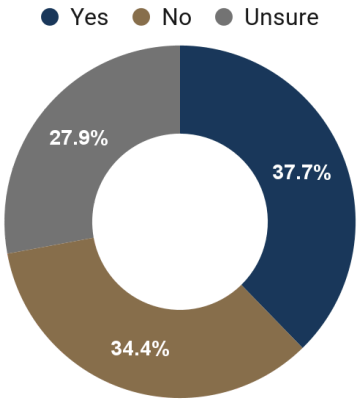
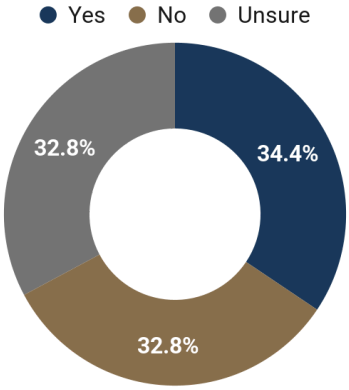


Chart 4: Survey Results - ERM Principles and Practices Training

Survey Question:
Have you and your team received any training on ERM principles and practices?



This indicates a gap between stated priorities, guiding documents, and practical implementation. There is an absence of formal mechanisms to consistently reinforce ERM behaviors and expectations beyond the broad statements found in strategic documents.

ERM EXPERTISE SUPPORT FOR RISK COMMITTEE

We interviewed a sample of Risk Committee members, ELT, and other City staff involved with ERM. Interview responses and survey data showed that although the Risk Committee is in place, the roles, expectations, and reporting lines are

insufficiently defined or understood, especially regarding how the committee supports strategic oversight. In addition, interviews with Risk Committee members indicated a need for more ERM expertise to support the committee's work.

This suggests that there may not be sufficient expertise on how to manage risk across the organization or how to implement ERM practices into various processes. This lack of knowledge could be mitigated by enhanced communication and education.

WHY THIS IS IMPORTANT

Clarity on ownership of the City's ERM program is crucial for its success. With appropriate seniority and authority clearly defined and communicated, the Deputy City Manager of Financial and Corporate Services is better equipped to oversee ERM practices City-wide and ensure appropriate frameworks for ERM-related activities are developed and used consistently and properly throughout the City.

In addition, defining and communicating ERM roles and responsibilities across all levels of the organization would enhance ERM capabilities and build a more broadly risk-aware culture.

Finally, dedicating resources towards increasing the level of ERM expertise and supporting the Risk Committee would aid in coordinating ERM activities, promoting consistency in ERM practices, and ensuring appropriate ERM communication flow throughout the City.

RECOMMENDATION 1

Enhance the Enterprise Risk Management Program to include:

- Updated documentation on the owner of the City's enterprise risk management program.
- A process to evaluate and track ERM maturity and lessons learned, and to implement refinements across the system.

- A communication strategy to ensure all staff levels receive timely and appropriate risk and performance information.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will:

- Develop a responsibility assignment matrix of leadership accountabilities. Additional accountability will be added as the system is developed, which will guide the targeted education required for Recommendation 2.
- Coordinate risk functions across the corporation to provide oversight on the implementation of policy and procedure C587A.
- Update the framework to reflect the owner as well as any necessary governance documents (for example, the terms of reference of the Risk Committee).
- Develop an ERM maturity assessment model to formally evaluate, on an ongoing basis, risk management practices across the organization. The model will be integrated within a broader strategic management assessment model, and will also help to address Recommendation 5. Assessing maturity will use a survey methodology, with

concrete scoring that can be used to introduce and report on system improvements.

- Provide decision-makers and employees at different levels with timely risk information in order to ensure information reaches the right people at the right time. Risk information will be part of an integrated system (Recommendations 5 & 6) that provides leaders with planning, performance and budget results to allow insight into progress on the City's strategic goals and operational and service priorities.

Implementation Date

June 30, 2027

RECOMMENDATION 2

Develop and implement ERM education that ensures employees are aware of their roles and responsibilities in ERM, including expectations to build a more broadly risk-aware culture and enhance ERM capabilities.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will:

- Develop and deliver ERM education and/or communication for branch managers and directors, to increase risk-awareness and accountability and enhance ERM capabilities in decision-making and service and operational management.
- Develop tailored education and/or communication materials for other employee groups as required.

Implementation Date

June 30, 2027

RECOMMENDATION 3

Dedicate resources towards increasing the level of ERM experience in the City, to assist in managing the ERM system and support the Risk Committee.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will:

- Hire a certified Risk Management professional to facilitate system oversight and coordination, promote consistent ERM practices and ensure appropriate ERM communication across the corporation.
- Monitor the resource allocation to ensure the program is adequately supported.

Implementation Date

March 31, 2026

Component 2: Strategy & Objective Setting - Initial Phase

COMPONENT AND PRINCIPLES

The Strategy & Objective Setting component focuses on aligning an organization's risk management practices with its overall strategy and objectives. It ensures that risk management is integrated into the strategic planning process and influences how objectives are set and risks are identified, assessed, and responded to.

This component requires defining a risk appetite, setting business objectives aligned with the strategy, and establishing a process for identifying and responding to risks. The crux of this component is defining risk appetite and tolerance thresholds, to determine how much risk an organization is willing to accept in the pursuit of its objectives.

Principles within the Strategy & Objective Setting component:

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Appendix B lists a detailed description of each of the principles.

KEY FINDINGS

We assessed the City to be in the Initial Phase for Strategy & Objective Setting.

We found that Council involvement in approving business plans ensures that strategic goals align with public policy mandates and that risk is a factor in major decisions. In addition, ELT interviewees confirmed that ELT members discuss strategy and risk at quarterly reviews providing a platform for integrated decision-making.

We also found that several City departments, including Integrated Infrastructure Services and Financial and Corporate Services, use environmental scanning practices to inform objective-setting and anticipate external risks.

However, the City does not have a documented methodology for defining and incorporating risk appetite and tolerance into its strategic decision-making processes. This means that it is unclear how much risk the City is willing to accept in the pursuit of its objectives.

We also found that despite structured strategic planning, few staff were able to articulate how risk informs the prioritization of business objectives. Formal risk profiling of alternative strategies is also limited. ERM's integration into planning is informal and inconsistent, lacking alignment with defined risk appetite. In addition, few departments proactively monitor evolving risks.

LACK OF CLEAR AND FORMALLY DEFINED RISK APPETITE

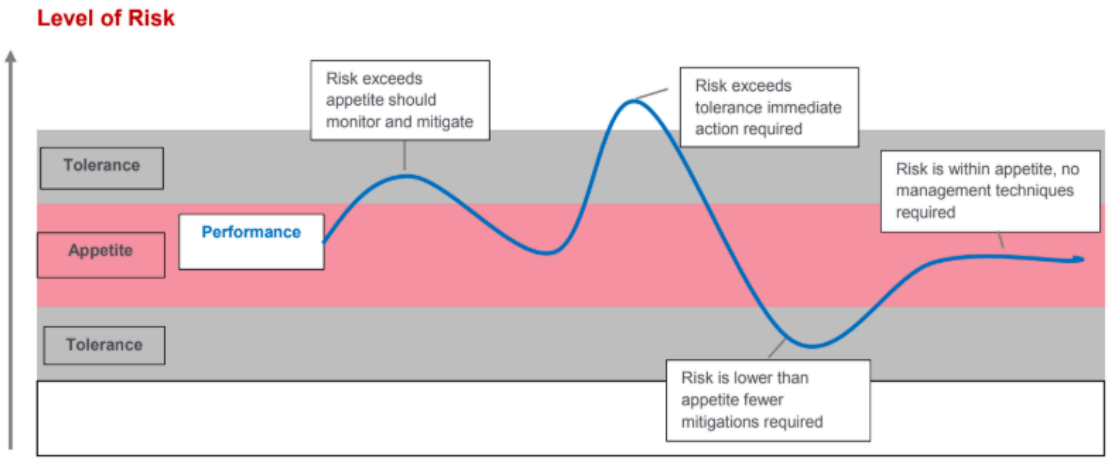
The City does not have clear and formally defined risk appetite statements and tolerance thresholds for each of its high-level risk categories.

Risk appetite refers to the amount and type of risk the organization is willing to accept in pursuit of its objectives. A defined risk appetite sets the point at which an organization would consider options for managing risk, such as:

- Avoiding the risk entirely.
- Setting controls and taking mitigation measures.
- Transferring the risks by some other means.

Risk tolerance determines the range of acceptable variation in risk (Figure 5).

Figure 5: Risk Appetite and Risk Tolerance[10]



DISCONNECT BETWEEN BUSINESS OBJECTIVES AND ACCEPTABLE RISK BOUNDARIES

The City engages in structured strategic planning anchored by Council leadership and guided by The City Plan and Corporate Business Plan. However, we found that few staff were able to articulate how risk informs prioritization of business objectives. While risk is acknowledged during planning, the evaluation of alternative strategies through structured risk profiling remains limited.

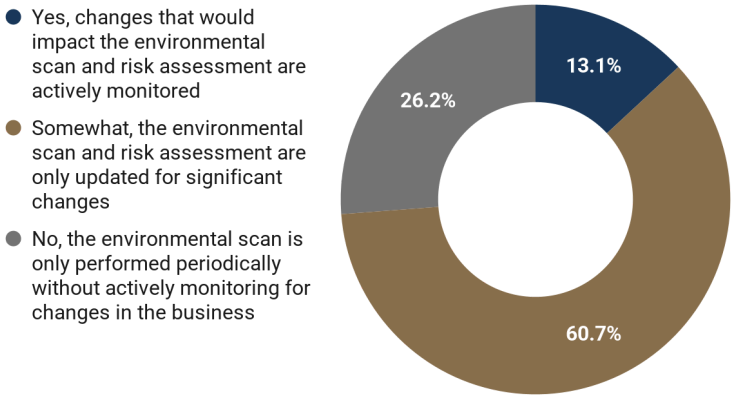
Senior leaders conceptually consider ERM, but its integration into planning decisions is informal and inconsistent; formal alignment of planning to risk appetite has not been established. As a result there could be a disconnect between the City's formulation of business objectives and staying within acceptable risk boundaries.

In addition, only 13.1 percent (8 of 61) of interview respondents indicated that their branch or section actively monitors changes in business context or emerging risks as part of ongoing planning. More than half of interview respondents (60.7 percent; 37 of 61) indicated that they only update risk registers reactively, in response to known events or once per year and not proactively as part of strategic planning (Chart 5).

[10] City of Calgary's Risk Appetite and Risk Tolerance 2019

Chart 5: Survey Results - Monitoring and Reassessment of Risk Assessments

Survey Question:
Does your branch/section actively monitor for and reassess the results of the risk assessment process for changes that would impact the environmental scan/business context that risks were assessed within?



WHY THIS IS IMPORTANT

Senior leaders and Risk Committee members widely acknowledged the need for a risk appetite framework. However, the absence of such a framework has resulted in inconsistent practices across the City and management decisions that often rely on individual interpretations of acceptable risk. This has led to inconsistent application and weakened alignment between ERM, strategy, and objective-setting. When strategies and objectives are not adequately informed by risk, the City's overall identification, assessment and responses to risks will be less effective and potentially misaligned with its true priorities.

RECOMMENDATION 4

As part of the City's Enterprise Risk Management Program, define the City's risk appetite and tolerance thresholds for each risk category.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will define and confirm risk appetites and thresholds for the City's eight risk categories. These will inform how risks are scored and monitored and will be used in decision-making**.**

Implementation Date

December 31, 2026

RECOMMENDATION 5

Develop consistent, city-wide methodologies for identifying, assessing, prioritizing, and responding to risks to formalize and integrate ERM practices. This includes applying risk appetite thresholds, ensuring real-time updates to risk registers, and linking ERM directly to business planning and corporate performance management and reporting.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will:

- Review and update ERM processes and tools to ensure effective identification, assessment, prioritization and responsiveness to risks. The Enterprise Risk Management Manual will be updated to reflect changes and be promoted as a learning and work resource for staff.
- Improve integration of all elements of the Strategic Planning Framework by connecting ERM processes, practices and information to planning, the responsibility matrix and performance reporting.

Implementation Date

December 31, 2026

Component 3: Performance - Preliminary Phase

COMPONENT AND PRINCIPLES

The performance component focuses on identifying, assessing, and responding to risks that may hinder an organization's ability to achieve its strategic and business objectives.

Performance involves prioritizing risks, selecting appropriate risk responses, and developing a portfolio view of risk, all while ensuring that effective monitoring and reporting of performance also takes place.

Principles within the Performance component:

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Appendix B lists a detailed description of each of the principles.

KEY FINDINGS

We assessed the City to be in the Preliminary Phase for Performance.

We found that ELT members and branch managers use performance reporting tools such as dashboards and performance measures to track business areas progress against business plans.

Several departments, including Integrated Infrastructure Services and Financial and Corporate Services, actively update their risk registers when performance targets are not met. In addition, the Service, Innovation and Performance Branch has systems in place to report aggregate performance indicators, which are used in risk prioritization discussions.

However, we also found that

- Risk identification and risk severity assessment practices lack uniformity across the City.
- Organizational performance reviews are often conducted in isolation from strategy, objective-setting and risk management, limiting feedback loops between outcomes, objectives, and risk exposure.

INCONSISTENT ERM PRACTICES

The City has established processes to identify risks through its ERM framework. These processes were established with contributions from senior leadership, Risk Committee, and operational staff. Branches use formal structures, including risk categories, risk registers, and heat matrices. However, risk identification practices are not yet applied uniformly across functions or leadership levels. Variability exists in terms of terminology, frequency of review, and the types of risks considered.

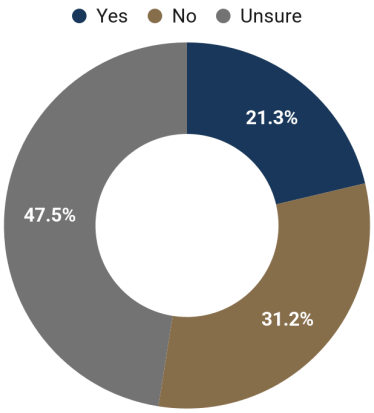
Furthermore, the City uses structured tools and scoring systems to assess the severity of risk, incorporating both impact and likelihood scoring to prioritize risk. However, inconsistencies exist in how time horizons are aligned with planning and how prioritization criteria are applied beyond severity. Residual risk is considered in many areas but lacks a citywide formal process. The interpretation of risk severity is influenced by staff experience, leading to subjectivity.

> *"There appears to be inconsistency in how risk is approached across the organization, with limited standardization or shared understanding. In some cases, staff may not have the capacity or see ERM as part of their daily responsibilities, especially when it feels disconnected from operational realities." - Survey Comment*

In addition, survey data highlights that respondents have some concerns about the integration of ERM in the corporation. A majority of survey respondents (78.7 percent; 48 out of 61)

indicated that they either don't believe or are unsure of whether the City has successfully integrated ERM activities within broader business, risk, and audit functions (Chart 6). These findings suggest that while intent and awareness are strong, the City's risk identification and assessment processes would benefit from standardization and consistency.

Chart 6: Integration of ERM Activities in Corporation



Survey Question:
In your opinion, has the City successfully integrated ERM activities within its broader business, risk, and audit functions?

WHY THIS IS IMPORTANT

Consistent ERM standards and practices across the organization will give leaders and all employees a common, comprehensive approach to managing risks. A consistent approach can also help senior leaders recognize the interconnectedness and potential impacts of risks across the entire organization. This approach allows for better understanding and management of complex risk scenarios across different business areas. In addition, consistent ERM practices promote transparency and accountability ensuring that all stakeholders are aware of potential risks and risk mitigation. This helps align risk management efforts with the City's strategic objectives.

RECOMMENDATION

See Recommendation 5

Component 4: Review & Revision - Preliminary Phase

COMPONENT AND PRINCIPLES

The Review & Revision component focuses on ensuring the effectiveness of an organization's ERM practices by regularly assessing and adapting them.

This component involves evaluating how well the ERM components are functioning over time, in light of changes to the organization's strategy, business objectives and the external environment. It also includes identifying areas for improvement and making necessary revisions to the ERM processes.

Principles within the Performance component:

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Appendix B lists a detailed description of each of the principles.

KEY FINDINGS

We assessed the City to be in the Preliminary Phase for Review & Revision.

We found that senior leadership reviews the City's risk register annually and quarterly and uses their findings to evaluate the City's overall risk portfolio. The Risk Committee provides structured oversight through annual reviews of corporate risk documentation. Some branches are beginning to explore advanced risk detection tools, including artificial intelligence pilots in environmental risk scanning. The City also evaluates entity and branch performance through structured plans and dashboard tools.

However, we also found that there is no formal, city-wide process for identifying and assessing internal and external changes that substantially impact the City's strategy or objectives. For the most part, change recognition is reactive and informal. While some performance evaluation processes are in place, integration of risk evaluation with risk management remains inconsistent. Many departments operate in silos, limiting the ability to connect performance deviations with risk reassessment or mitigation strategies.

We also found that ERM program improvements are not supported by structured evaluation tools or feedback loops, relying instead on ad hoc leadership initiatives. None of the interviewees referenced existing tools, processes, or roles that serve to evaluate the effectiveness of ERM practices or capture lessons learned for future enhancement.

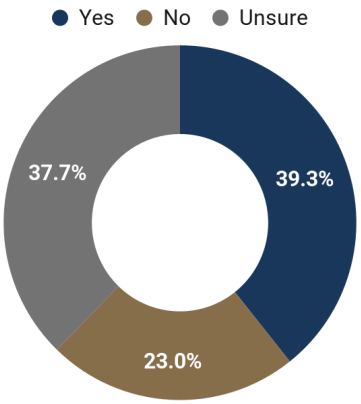
LACK OF FORMAL PROCESS TO PROACTIVELY IDENTIFY AND ASSESS CHANGES ACROSS THE CITY

The City acknowledges that shifts in the internal and external environment may affect the achievement of strategic and business objectives. However, the City does not have a formal process in place to proactively identify or assess such changes across the City. Risk re-assessment practices are typically reactive, with limited standardization or continuous monitoring, resulting in inconsistent responsiveness to substantial shifts in business context. While some areas respond to major changes through ad hoc discussions or scheduled reviews, proactive scanning and formal trigger-based risk re-assessments are limited.

Interview respondents indicated that change recognition is largely informal, occurring through meetings or ad hoc discussions. In addition, only 39.3 percent (24 of 61) of survey respondents indicated that their branch or section has a process to periodically review risks (Chart 7).

Chart 7: Survey Results - Periodic Review of Risks

Survey Question:
Do you have a process to review risks in your branch/section periodically?



LACK OF ERM MONITORING

The City does not have a formal process to evaluate or improve its ERM program or practices. We found that efforts are informal, reactive, and dependent on individual leadership rather than institutionalized systems. While individual leaders acknowledge the importance of ERM and continuous improvement, implementation is limited by an absence of formal processes and dedicated ownership.

Efforts to advance ERM are further hindered by resource constraints, the absence of formal feedback loops, and a critical loss of leadership continuity. High turnover across the Risk Committee, Service, Innovation and Performance Branch staff, and leadership ranks have diluted institutional knowledge and weakened follow-through on ERM initiatives. Without consistent evaluative mechanisms, capacity planning, or governance structures to support ERM enhancement, the City's ERM system risks stagnation and the City may struggle to adapt its risk profile over time in alignment with evolving business objectives.

WHY THIS IS IMPORTANT

A formal process to evaluate ERM would ensure that the City's ERM is not a static exercise but a dynamic system that evolves with the organization and its environment, and drives continuous improvement and strategic resilience. Without monitoring to assess the effectiveness of its ERM program, the City will be unable to track how risks are evolving and how the

broader risk management is performing.

RECOMMENDATION

See Recommendation 1

Component 5: Information, Communication & Reporting- Preliminary Phase

COMPONENT AND PRINCIPLES

The Information, Communication, and Reporting component emphasizes the importance of timely and relevant information flow within an organization for effective internal control.

This component includes obtaining, generating, and using information from internal and external sources, as well as communicating that information effectively to relevant parties.

Principles within the Information, Communication & Reporting component:

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Appendix B lists a detailed description of each of the principles.

KEY FINDINGS

We assessed the City to be in the Preliminary Phase for Information, Communication & Reporting.

We found that high-level considerations of strategic risks are communicated to Council and ELT in formal reports. For example, The City Plan and corporate business plans communicate the City's strategic direction and overall risk posture. These reports also identify the City's overall approach to managing risk and aligning risk management, with the City's strategic direction. In addition, the Service, Innovation and Performance Branch employs a cascading communication model using newsletters and meetings to share ERM system updates across operational levels.

However, we found that information and technology systems to support ERM are underdeveloped and inconsistently applied across the City. While pockets of innovation exist, such as dashboard visualizations, most risk processes remain manual and siloed. Furthermore, data governance structures for ERM reporting are not clearly defined and the City has no centralized system in place to consolidate risk insights.

Although the City has some communication mechanisms for ERM, we found that the City lacks an effective communication strategy to ensure relevant and timely risk information reaches the right people at the right time. This includes a deficiency in communicating employee expectations regarding ERM and performance management, resulting in a lack of clarity on individual roles and responsibilities and inconsistent accountability for risk management.

Furthermore, the City's current ERM reporting systems appear fragmented, with uneven distribution of risk and business performance information and varying degrees of familiarity with available tools.

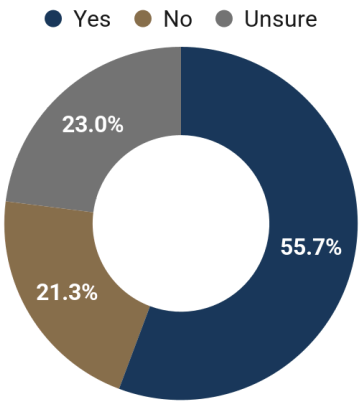
INCONSISTENT USE OF TECHNOLOGY IN ERM PROCESS

We found that information and technology systems to support ERM are underdeveloped and inconsistently applied across the City. The City's current risk management practices are primarily facilitated by manual tools such as Google Sheets, supplemented in some areas by dashboards and visualization platforms. While pockets of innovation exist, most risk processes remain manual and siloed. The reliance on basic tools like spreadsheets limits scalability, consistency, and timeliness in risk reporting.

Survey responses confirm that analytic capabilities are not yet consistently embedded in organizational culture or practice. Only 55.7 percent (34 of 61) of respondents affirmed the use of data analytics for risk-related purposes (Chart 8).

Chart 8: Survey Results - Use of Data Analytics

Survey Question:
Does your branch/section use data analytics to identify risks, reduce existing risk, and identify trends?



A more integrated, standardized, and strategically governed approach to ERM technology is needed to improve data-driven risk oversight and decision-making. ***(See Recommendation 6)***

LACK OF EFFECTIVE COMMUNICATION OF RISK INFORMATION

Effective communication of risk information ensures that individuals at all levels of the City, along with external stakeholders, receive timely, relevant, and understandable insights to support effective decision-making and risk management. The City communicates its strategy, business objectives, and risk-related information through a combination of formal reports, meetings, and informal discussions. Communication about ERM occurs internally across multiple organizational levels and to interested parties such as the City Council and the public.

Although the City has some communication mechanisms for ERM, we found that the City lacks an effective communication strategy to ensure relevant and timely risk information reaches the right people at the right time. Including but not limited to information about expectations of employees in relation to ERM and performance management, so that employees at all levels understand their individual roles and responsibilities. The City has no framework for linking ERM responsibilities, accountability structures and employee performance

expectations. This gap leads to inconsistency in accountability for risk management. ***(See Recommendation 1)***

PERCEIVED GAPS IN RISK AND PERFORMANCE REPORTING

Formal reporting mechanisms at the City include presentations such as the Annual Corporate Strategic Risk reports. These documents are presented to the ELT, the Risk Committee, and Council. These reports, according to the Risk Committee Co-Chair, aim to guide business planning, budgeting, and operational goal setting, while also informing the Council of capacity constraints and high-risk areas that may require mitigation strategies.

However, interview and survey responses suggest inconsistent dissemination or understanding of these reports across the broader organization. While these documents are shared at the senior level, their visibility and influence at the branch and director level are uncertain. There is no assurance that this information effectively cascades through all levels of the City.

The supporting survey data confirms that although many staff receive some information on risk and performance, a majority do not feel well-informed. Directors reported significant gaps in receiving complete or timely information on key ERM elements. Only about a quarter of directors surveyed feel they receive adequate information on identified risks and risk assessments. This drops to about 12% for both risk responses and performance results (Chart 9). In comparison, 79% (15 out of 19) branch managers indicated they receive all the risk information they require, but only 32% (6 out of 19) indicated they receive the performance information they require.

Chart 9: Survey Results - Risk and Performance Reporting

Survey Question:
Do you feel you receive adequate information related to?

The City's current reporting systems appear fragmented, with uneven distribution of risk and performance information and varying degrees of familiarity with available tools. Enhanced communication pathways, stronger role-based dissemination practices, and broader visibility into risk reporting documents are needed to strengthen citywide risk culture and strategic alignment. ***(See Recommendation 1)***

WHY THIS IS IMPORTANT

For ERM to be effective, relevant and timely risk information must reach the right people at the right time. An effective communication strategy supported by technology would provide leaders, managers, and staff with the necessary data to make informed decisions. Without this timely delivery of useful information, decisions might be made in a vacuum, leading to misalignment with the City's strategic goals. In addition, effective communication and targeted ERM training would foster a risk aware culture and drive accountability for risk management.

RECOMMENDATION 6

Improve ERM's technology infrastructure to support centralized risk documentation and reporting.

Responsible Party

Chief Financial Officer and Deputy City Manager, Financial and Corporate Services Department

Accepted

Management Response

Administration will enhance the ability to gather, store and communicate risk information through centralized risk documentation and reporting. This will be part of a broader system that connects risks to planning and performance information, to improve decision-making by leaders.

Implementation Date

December 31, 2026

ACKNOWLEDGEMENT

We would like to thank all the staff and management we dealt with for their cooperation during this audit.

Appendix A – ERM Maturity Assessment Rating Model

	Initial *Level 1*	Preliminary *Level 2*	Defined *Level 3*	Integrated *Level 4*	Optimized *Level 5*
Governance & Culture	• No formal governance policies. • No risk management documentation. • Oversight, roles, and responsibilities are unclear. • Risk culture is weak and talent management lacks structure.	• Governance policies exist but are not consistently documented or enforced. • Roles are loosely defined. • Risk awareness is emerging. • Basic talent management policies are in place but lack strategic alignment.	• Documented governance policies and procedures define board and management roles. • Risk culture is supported through formal policies. • Talent management is structured to align with risk-informed decision-making.	• Governance policies are regularly reviewed and updated, ensuring alignment with business strategy and risk management objectives. • A strong risk-aware culture is embedded in decision-making and performance evaluation.	• Governance and risk culture policies are continuously improved and dynamically adjusted. • Talent management integrates real-time risk considerations. • Leadership actively fosters risk-informed growth.
Strategy & Objective Setting	• No formal documentation of business context and risk considerations in strategy and business objective-setting. • Risk appetite and tolerance are loosely defined.	• Some risk-related strategy documents exist, but they are incomplete, not formally approved, or inconsistently applied. • Strategy and business objectives do not align with risk appetite or tolerance.	• Formalized ERM policies ensure risk appetite/tolerance and strategy- and business objective-setting are documented and reviewed. • Strategy and business objectives align with risk considerations.	• Risk considerations are fully documented and integrated into decision-making. • Strategy, business objectives, strategy, and risk appetite/tolerance are regularly evaluated against changing conditions.	• Continuous improvement of documentation linking strategy/business objectives with risk ensures agile risk-informed decision-making. • Advanced analytics and scenario planning enhance strategy alignment.
Performance	• No formal documentation exists for risk identification, assessment, prioritization, or response planning. • Risks are handled reactively.	• Some risk documentation is in place. • Risk assessments and prioritization are inconsistent. • No standardized procedures for risk response.	• Documented risk identification and assessment procedures are established. • Risk prioritization follows a defined framework. • Responses are systematically documented.	• Risk assessment, response, and portfolio management policies are fully documented, integrated, and actively monitored for compliance.	• Risk management documentation is continuously refined and linked to predictive analytics. • Risk management is leveraged for real-time, data-driven decision-making.
Review & Revision	• No formal ERM review or revision policies. • Changes in risk profile and impact on business strategy and objectives are not assessed systematically.	• Some review mechanisms exist, but they are not formally documented or systematically applied. • Performance evaluation is not risk informed.	• Periodic risk reviews are documented and required. • ERM effectiveness is assessed using standardized evaluation criteria.	• ERM review and revision policies are embedded in business processes, ensuring continuous monitoring and improvement. • Risk-related performance evaluations are required.	• ERM review policies are dynamic and continuously improved. • Automated risk monitoring enables real-time insights for decision-making.
Information, Communication, & Reporting	• No formal documentation exists for risk communication, reporting, or information management. • Risk data is not shared systematically.	• Some risk reporting processes are in place, but they are not well documented or consistently followed. • Communication is informal.	• Formalized risk reporting policies and communication channels exist, ensuring transparency and structured information flow.	• Risk communication and reporting policies are standardized, embedded, and actively used for decision-making at all levels.	• Automated, real-time risk reporting and advanced analytics drive strategic insights. • Risk communication is proactive and fully aligned with business needs.

Appendix B – ERM Components and Principles[11]

Governance & Culture

1. **Exercises Board Risk Oversight** —The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures** —The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture** —The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values** —The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals** —The organization is committed to building human capital in alignment with the strategy and business objectives.

Strategy & Objective-Setting

6. **Analyzes Business Context** —The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite** —The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies** —The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives** —The organization considers risk while establishing the business objectives at various levels that align and support strategy.

Performance

10. **Identifies Risk** —The organization identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses Severity of Risk** —The organization assesses the severity of risk.
12. **Prioritizes Risks** —The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses** —The organization identifies and selects risk responses.
14. **Develops Portfolio View** —The organization develops and evaluates a portfolio view of risk.

[11] COSO, *Enterprise Risk Management: Integrating Strategy and Performance* (2017)

Review & Revision

15. **Assesses Substantial Change** —The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews Risk and Performance** —The organization reviews entity performance and considers risk.
17. **Pursues Improvement in Enterprise Risk Management** —The organization pursues improvement of enterprise risk management.

Information, Communication & Reporting

18. **Leverages Information and Technology** —The organization leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates Risk Information** —The organization uses communication channels to support enterprise risk management.
20. **Reports on Risk, Culture, and Performance** —The organization reports on risk, culture, and performance at multiple levels and across the entity.