CITY OF MEDICINE HAT

Policy

Medicine Hat

Title: ENTERPRISE RISK MANAGEMENT POLICY			Number: 0184
Reference: N/A Administrative Committee - October 3, 2024 Audit Committee - October 23, 2024	**Adopted by City Council:** November 4, 2024		**Supersedes:** N/A
	City Clerk	**City Manager**	
Prepared by: CORPORATE PLANNING AND PERFORMANCE			

STATEMENT

THE ENTERPRISE RISK MANAGEMENT (ERM) POLICY FOR THE CITY OF MEDICINE HAT (CITY) ESTABLISHES A STRUCTURED AND COMPREHENSIVE APPROACH TO MANAGING RISKS ACROSS THE ORGANIZATION. THIS POLICY ENSURES THAT RISK MANAGEMENT IS INTEGRATED INTO ALL OPERATIONS, FOSTERING A CULTURE OF RISK AWARENESS AND RESILIENCE THROUGHOUT THE ORGANIZATION.

ALIGNED WITH THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO) ENTERPRISE RISK MANAGEMENT (ERM) 2017 FRAMEWORK AND THE ISO 31000:2018 RISK MANAGEMENT STANDARDS, THE POLICY PROVIDES A ROBUST FRAMEWORK FOR IDENTIFYING, ASSESSING, MITIGATING, AND MONITORING BOTH DOWNSIDE AND UPSIDE RISKS. BY ADOPTING BEST PRACTICES, THE CITY STRIVES TO ENHANCE ITS ABILITY TO RESPOND TO UNCERTAINTIES WHILE LEVERAGING OPPORTUNITIES (UPSIDE RISK) TO MEET ITS STRATEGIC OBJECTIVES.

THE CITY'S RISK MANAGEMENT GOVERNANCE INCLUDES OVERSIGHT BY SENIOR LEADERSHIP, ENSURING ACCOUNTABILITY ACROSS ALL DEPARTMENTS. CONTINUOUS REVIEW AND IMPROVEMENT OF THE RISK MANAGEMENT PROCESS ENSURE THAT RISKS ARE ACTIVELY MANAGED AND COMMUNICATED TO SUPPORT INFORMED DECISION-MAKING.

THIS POLICY IS ESSENTIAL FOR EFFECTIVE RESOURCE ALLOCATION, COMPLIANCE WITH LEGAL AND REGULATORY STANDARDS, SAFEGUARDING THE CITY'S ASSETS AND REPUTATION, AND MEETING STAKEHOLDER EXPECTATIONS. IT ALSO PROMOTES TRANSPARENCY IN RISK REPORTING AND DECISION-MAKING, SUPPORTING INNOVATION AND THE LONG-TERM SUSTAINABILITY OF THE CITY'S OPERATIONS.

BY EMBEDDING ERM PRINCIPLES INTO ITS DAY-TO-DAY ACTIVITIES, THE CITY NOT ONLY AIMS TO PROTECT PUBLIC TRUST, DELIVER EFFECTIVE SERVICES, AND CONTRIBUTE TO THE WELL-BEING OF ITS COMMUNITY, BUT ALSO RECOGNIZES THAT THIS POLICY IS PIVOTAL FOR THE LONG-TERM SUSTAINABILITY AND SUCCESS OF THE ORGANIZATION.

1. AUTHORITY

1.1 Pursuant to Section 201 of the Municipal Government Act (Alberta), Council is responsible for developing and evaluating the policies of the City. Pursuant to Section 207 of the Municipal Government Act (Alberta), the City Manager is responsible for ensuring that the policies of the City are implemented.

1.2 Administrative Committee
The procedural authority responsible for overseeing and guiding administrative processes.

1.3 Managing Director, Corporate Services & Chief Financial Officer (or delegate)
(a) Has implementation authority to:
  (i) Develop and administer practices, systems and controls for the City's ERM program.
  (ii) Monitor compliance with the City's ERM program.
  (iii) Report to the Audit Committee on an annual basis on the City's ERM activities, including the annual ranking of enterprise level risks by the Executive Leadership Team (ELT).

2. DEFINITIONS

2.1 Emerging Risk – a new or unforeseen risk that hasn't yet been contemplated.

2.2 Enterprise Risk (ER) – major risk (also known as strategic risk) that can potentially hinder the ability of the City of Medicine Hat (City) to achieve its corporate/ strategic objectives.

2.3 Enterprise Risk Management (ERM) – a systematic and integrated process designed to identify, assess, manage, mitigate, and monitor critical risks that could significantly impact the City's ability to achieve its objectives.

2.4 Enterprise Risk Register (ERR) – a detailed repository that catalogs identified risks, including their descriptions, potential impacts, risk ratings, and assigned risk owners. It functions as a central tool for effective risk monitoring and management.

2.5 ERM Activities (Activities) – actions taken to mitigate specific risks and reduce their impact on the City.

2.6 ERM Committee (Committee) – members of the Executive Leadership Team (ELT) and Senior Leadership Team (SLT), risk owners and other stakeholders, whose purpose is to provide guidance on matters relating to the City's ERM framework.

2.7 ERM Framework (Framework) – a structured and comprehensive system implemented by the City to identify, assess, manage, and monitor risks, ensuring alignment with strategic goals and enhancing its ability to achieve its objectives.

2.8 Executive Leadership Team (ELT) – the City Manager, their direct reports, and the Police Chief, or delegates.

2.9 Impact – the potential positive or negative consequence of a risk on the organization's strategy or business objectives, affecting its ability to achieve its goals.

2.10 Inherent Risk – the level of risk arising from internal and external factors before any controls or mitigation measures are applied. It represents the raw, uncontrolled risk associated with a particular situation or activity.

2.11 Key Results Indicators (KRI) – a metric that measures the quantitative results of the City's actions to track progress in reaching its strategy.

2.12 Key Risk – a critical risk identified in the risk register that poses the greatest threat to the City's ability to achieve its strategic goals and requires prioritized attention and management due to its potential severity, likelihood, or both.

2.13 Likelihood – the possibility that a given event will occur.

2.14 Mitigation – the act or process of reducing the severity, impact, or likelihood of risks.

2.15 Objectives – measurable steps the City takes to achieve its strategy.

2.16 Operational Risk – a risk that impacts specific departments or functions within the organization and may affect broader organizational objectives if not managed and escalated appropriately.

2.17 Operational Risk Register – risks that primarily affect specific departments but may not impact the entire organization unless escalated. These risks should be documented in each department's Operational Risk Register.

2.18 Opportunity Risk – the potential for beneficial outcomes or gains arising from managing risks (sometimes referred to as Upside Risk or Positive Risk).

2.19 Residual Risk – the portion of inherent risk that remains after execution of risk responses/ mitigation (sometimes referred to as net risk).

2.20 Risk – the possibility that events will occur and impact the City's achievement of strategy and objectives.

2.21 Risk Appetite (Appetite) – the type and level of risk that the City is willing to accept in pursuit of its corporate/ strategic objectives.

2.22 Risk Capacity – the maximum amount of risk that the City can absorb in the pursuit of strategy and objectives.

2.23 Risk Category – the accumulation of risks of a shared characteristic into a single category with a common risk appetite.

2.24 Risk Owner – an employee identified as the appropriate person to monitor, manage, or mitigate an identified risk for the City.

2.25 Risk Profile – a comprehensive overview of the risks associated with a particular level or aspect of the City's operations. It considers the types, severity, and interrelationships of these risks, and their potential impact on organizational performance relative to strategic goals and objectives.

2.26 Senior Leadership Team (SLT) – the City Manager, their direct reports, Directors, and the Fire Chief, or delegates.

2.27 Strategy – the City's plan to achieve its mission and vision and apply its core values.

2.28 Target – the specific outcome or goal that the City aims to achieve through its strategic efforts and initiatives.

2.29 Tolerance – the permissible range of deviation from expected performance levels in relation to achieving set objectives for the City.

2.30 Trending Risk – a significant and emerging risk that is currently affecting similar organizations and is gaining attention due to its increasing relevance and impact.

3. PRINCIPLES

3.1 Integration
Embedding risk management into the organization's processes and decision-making.

3.2 Comprehensiveness
Identifying and managing all types of risks, both internal and external, that could impact the City's objectives.

3.3 Accountability
Defining clear roles and responsibilities for risk management throughout the City.

3.4 Communication
Ensuring transparent and timely reporting of risk identification and management to relevant stakeholders.

3.5 Continuous Improvement
Regularly reviewing and improving the risk management framework and practices.

4. ROLE OF COUNCIL

4.1 To receive, review and adopt this policy and any recommended amendments thereto.

4.2 Ensure Audit Committee's mandate to provide oversight and adequacy of the overall ERM framework.

5. ROLE OF CITY MANAGER

5.1 The City Manager is responsible for executing this policy, including the establishment of appropriate procedures to ensure its effective implementation.

5.2 Serves as the ERM champion, overseeing the implementation of the ERM program, delegating responsibilities to ensure effective execution, and ensuring that the program is regularly reviewed and updated.

5.3 Provides strategic direction and approves the governance structure to ensure an effective and efficient ERM process.

CITY OF MEDICINE HAT

Procedure

Medicine Hat

Title: ENTERPRISE RISK MANAGEMENT	Number: 0184

Approved by the Administrative Committee: May 27, 2026		Supersedes: Procedure 0184: October 3, 2024
City Clerk	City Manager	
Prepared by: Finance Department		

1. DEFINITIONS

1.01 Emerging Risk – a new or unforeseen risk that hasn't yet been contemplated.

1.02 Enterprise Risk (ER) – major risk (also known as strategic risk) that can potentially hinder the ability of the City of Medicine Hat (City) to achieve its corporate/ strategic objectives.

1.03 Enterprise Risk Management (ERM) – a systematic and integrated process designed to identify, assess, manage, mitigate, and monitor critical risks that could significantly impact the City's ability to achieve its objectives.

1.04 Enterprise Risk Register (ERR) – a detailed repository that catalogs identified risks, including their descriptions, potential impacts, risk ratings, and assigned risk owners. It functions as a central tool for effective risk monitoring and management.

1.05 ERM Activities (Activities) – actions taken to mitigate specific risks and reduce their impact on the City.

1.06 ERM Committee (Committee) – members of the Executive Leadership Team (ELT) and the Senior Leadership Team (SLT), risk owners and other stakeholders, whose purpose is to provide guidance on matters relating to the City's ERM framework.

1.07 ERM Framework (Framework) – a structured and comprehensive system implemented by the City to identify, assess, manage, and monitor risks, ensuring alignment with strategic goals and enhancing its ability to achieve its objectives.

1.08 Executive Leadership Team (ELT) – the City Manager and their direct reports or delegates.

1.09 Fraud – an intentional deception used to secure an unfair or unlawful gain, including but not limited to:

(a) forgery or unauthorized or inappropriate alteration of a cheque, bank draft, financial document; or any other document belonging to the City;

(b) impropriety in the handling or reporting of money or financial transactions;

(c) misrepresentation, misappropriation, misuse or attempted misuse, or unauthorized destruction of City Assets;

(d) profiteering as a result of insider knowledge of City activities;

(e) disclosing confidential and proprietary information to outside parties;

(f) deception involving procurement, contracting, or vendor relationships, including bid-rigging, collusion, kickbacks, or falsification of procurement documents;

(g) falsification or manipulation of City records, data, reports, permits, inspections, or timekeeping information;

(h) undisclosed or improper conflicts of interest;

(i) unauthorized use or misuse of City services, systems, or network access;

(j) soliciting or accepting for private gain, money, gifts, favours, or services from any individual, organization, or business undertaking, doing, or seeking to do, business with the City other than gifts, favours, or services given:

(i) as an exchange of hospitality that is reasonable in the course of a municipal government's business, or

(ii) as a ceremonial presentation to a person acting in a representative capacity on behalf of the City; and

(k) any similar or related inappropriate conduct.

1.10 Impact – the potential positive or negative consequence of a risk on the organization's strategy or business objectives, affecting its ability to achieve its goals.

1.11 Inherent Risk – the level of risk arising from internal and external factors before any controls or mitigation measures are applied. It represents the raw, uncontrolled risk associated with a particular situation or activity.

1.12 Key Results Indicators (KRI) – a metric that measures the quantitative results of the City's actions to track progress in reaching its strategy.

1.13 Key Risk – a critical risk identified in the risk register that poses the greatest threat to the City's ability to achieve its strategic goals and requires prioritized attention and management due to its potential severity, likelihood, or both.

1.14 Likelihood – the possibility that a given event will occur.

1.15 Mitigation – the act or process of reducing the severity, impact, or likelihood of risks.

1.16 Objectives – measurable steps the City takes to achieve its strategy.

1.17 Operational Risk – a risk that impacts specific departments or functions within the organization and may affect broader organizational objectives if not managed and escalated appropriately.

1.18 Operational Risk Register – risks that primarily affect specific departments but may not impact the entire organization unless escalated. These risks should be documented in each department's Operational Risk Register.

1.19 Opportunity Risk – the potential for beneficial outcomes or gains arising from managing risks (sometimes referred to as Upside Risk or Positive Risk).

1.20 Residual Risk – the portion of inherent risk that remains after execution of risk responses/ mitigation (sometimes referred to as net risk).

1.21 Risk – the possibility that events will occur and impact the City's achievement of strategy and objectives.

1.22 Risk Appetite (Appetite) – the type and level of risk that the City is willing to accept in pursuit of its corporate/ strategic objectives.

1.23 Risk Capacity – the maximum amount of risk that the City can absorb in the pursuit of strategy and objectives.

1.24 Risk Category – the accumulation of risks of a shared characteristic into a single category with a common risk appetite.

1.25 Risk Owner – an employee identified as the appropriate person to monitor, manage, or mitigate an identified risk for the City.

1.26 Risk Profile – a comprehensive overview of the risks associated with a particular level or aspect of the City's operations. It considers the types, severity, and interrelationships of these risks, and their potential impact on organizational performance relative to strategic goals and objectives.

1.27 Senior Leadership Team (SLT) – the City Manager, their direct reports, Directors, the Fire Chief, and Police Chief, or delegates.

1.28 Strategy – the City's plan to achieve its mission and vision and apply its core values.

1.29 Target – the specific outcome or goal that the City aims to achieve through its strategic efforts and initiatives.

1.30 Tolerance – the permissible range of deviation from expected performance levels in relation to achieving set objectives for the City.

1.31 Trending Risk – a significant and emerging risk that is currently affecting similar organizations and is gaining attention due to its increasing relevance and impact.

2. RESPONSIBILITIES

2.02 City Council

(a) City Council (Council) is the approving authority and will:

(i) Receive, review and adopt this policy and any recommended amendments thereto.

(ii) Mandate the Audit Committee to provide oversight, and ensure adequacy, of the overall framework.

2.03 Audit Committee

(a) The committee has the oversight authority to provide overall adequacy of the framework, and will:

(i) Receive, and communicate to City Council, the results of the ERM activities.

(ii) Communicate framework and procedures (or protocols) to members of Council.

(iii) Obtain and review periodically, risk reports of the City to determine that risks are identified and managed appropriately.

(iv) Review and approve the risk framework to be implemented by City administration.

2.04 Administrative Committee

(a) The Administrative Committee has the procedural authority to:

(i) Review and approve the ERM framework and procedures and recommend amendments to the policy to Council through the Audit Committee.

(ii) Ensure ERM practices are aligned with the City's strategic objectives and regulatory requirements.

(iii) Oversee the identification, assessment, and management of key enterprise risks.

(iv) Monitor the effectiveness of risk mitigation strategies and recommend necessary adjustments.

(v) Provide guidance on the reporting of key risks to senior leadership and ensure proper communication of ERM activities across the organization.

2.05 City Manager

(a) The City Manager has executive authority and will:

(i) Act as the ERM champion and commission others to deliver on the program, ensuring that it is actively reviewed.

(ii) Provide direction and approve the governance structure for an effective ERM process.

2.06 Managing Director, Corporate Services & Chief Financial Officer (or delegate)

(a) The managing director is responsible for implementation and has the authority to:

(i) Develop and administer practices, systems and controls for the City's ERM program.

(ii) Monitor compliance with the City's ERM program.

(b) and will:

(i) Report to the Audit Committee on an annual basis on the City's ERM activities, including ELT's annual ranking of enterprise level risks.

2.07 Finance Department

(a) The department is responsible for:

(i) Developing and maintaining procedural documents that support the implementation and management of the ERM framework.

(ii) Collaborating with risk owners to ensure consistent application of ERM processes across departments.

(iii) Facilitating risk assessments and reviews, providing guidance on best practices for risk identification, mitigation, and monitoring.

(iv) Monitoring the effectiveness of risk management activities and reporting on performance against risk management objectives.

(v) Ensuring alignment between risk management activities and the City's strategic goals and objectives.

(vi) Ensuring that business units embed ERM principles into their objectives, strategies, and day-to-day operations.

2.08 Executive Leadership Team

(a) ELT is responsible for:

(i) Review overall adequacy of the ERM Framework.

(ii) Approve risk assessment findings for subsequent Audit committee meetings.

(iii) Recommends the risk appetite for each identified enterprise risk to Council.

(iv) Monitor each identified enterprise risk, while considering the approved risk appetite.

(v) Assign identified enterprise risks to risk owners for analysis, management and mitigation.

(vi) Annually rank the enterprise level risks.

(vii) Annually review risk appetite for each identified enterprise risk.

2.09 Risk Owner

(a) The risk owner:

(i) Assumes ownership to manage and mitigate assigned enterprise risks by developing and implementing practices, systems, and controls to address the risks. This may include developing comprehensive programs to manage their risks with oversight from an appropriate committee.

(ii) Reviews reports from the ERM Committee and presents risk reports to the ELT.

2.10 Enterprise Risk Management Committee

(a) The committee has oversight for the management of enterprise risks, and will:

(i) Ensure that risk management practices are effectively integrated into the organization’s strategy and operations.

(ii) Include identifying and recommending risks for the ERR.

(iii) Liaise between Risk Owners in managing and reporting enterprise risks and considering information on trending and emerging risks.

(iv) Review and monitor the risk profile, and advise on risk mitigation strategies, ensuring that risks are managed to protect and enhance organizational value.

(v) Promote compliance with the ERM policy, procedures, and framework.

(vi) Report regularly, conduct analysis, and make recommendations to the ELT on the management and mitigation of identified enterprise risks.

(vii) Engage any other City Committees to monitor the City’s management of enterprise risks, considering the approved risk appetite, as appropriate.

2.11 Enterprise Risk Management Manager

(a) The ERM manager:

(i) Is responsible for implementation, monitoring and reporting.

(ii) Develops ERM standards, processes and best practices.

(iii) Creates and maintains ERM tools and templates, including risk categories, risk heat maps and risk rating tables.

(iv) Establishes and updates a register of identified enterprise risks.

(v) Provides training and advice on the City's ERM program to Risk Owners and others involved in the City's activities.

(vi) Prepares reports for review by the Audit Committee, ELT, SLT and the ERM Committee, as needed.

2.12 Employees of the City of Medicine Hat

(a) All City employees are required to:

(i) Support the ERM program by assisting in identifying, analyzing, evaluating, and treating potential enterprise risks.

(ii) Familiarize themselves with the ERM program to ensure that the enterprise risks arising from the strategic or operational decisions are appropriately managed and align with the ERM program and the City's risk appetite.

(iii) Apply sound enterprise risk management.

(iv) Report risks with causes, impacts or mitigation beyond and within their scope of responsibility to the ERM Committee.

3. PROCEDURES

3.01 Risk Identification

Recognize potential risks that could impact City operations, confidentiality, or service delivery by:

(a) Conducting regular risk assessments involving key stakeholders (e.g., directors, department heads, etc.), using tools such as risk registers, surveys, and workshops to gather input on potential threats, including fraud.

(b) Identifying emerging and trending risks (e.g., regulatory changes, cybersecurity threats, data breaches, supply chain disruptions, etc.) and their potential impact on City operations.

(c) Categorizing identified risks (strategic, operational, reputational, fraud, etc.) to streamline assessment, prioritization, and mitigation efforts.

(d) Documenting identified risks in a centralized risk register with assigned ownership, timelines for review, and ongoing updates based on new insights.

(e) Aligning identified risks with the City's strategic objectives to ensure that risk management supports long-term organizational goals.

(f) Utilizing Key Risk Indicators (KRIs) to monitor and flag potential risks in real-time, allowing for a proactive management approach.

3.02 Perform Environmental Scans

Proactively identifying processes and procedures followed by other municipalities, cities, etc. through:

(a) Conducting regular environmental scans (e.g., annually or biannually) to identify trends, emerging risks. This can include reviewing industry reports, government regulations, healthcare trends, and cybersecurity developments.

(b) Engaging with external experts and thought leaders to gain insights into potential new risks (e.g., pandemic response, evolving data protection laws, and public health challenges).

(c) Analyzing changes in the external environment, such as technological advancements, political developments, and societal shifts, that could pose risks to CMH operations or compliance.

(d) Regularly updating the risk register with emerging risks and ensuring mitigation strategies are developed in advance.

3.03 Best-in-Class Practices

Ensure that CMH adopts leading industry standards and methodologies for effective risk management by:

(a) Benchmarking CMH's risk management practices against best-in-class frameworks from recognized organizations (e.g., COSO, ISO 31000, or NIST for cybersecurity).

(b) Collaborating with peer institutions and industry associations to share best practices and lessons learned in risk management.

(c) Reviewing case studies of successful risk management initiatives from other cities or municipalities to identify areas for improvement.

(d) Use scenario planning and forecasting models to simulate potential impacts of these emerging risks.

(e) Regularly update the risk register with emerging risks and ensure mitigation strategies are developed in advance.

3.04 Risk Appetite

(a) Define the level of risk that the City is willing to accept for each risk category, aligning with City Council's strategic objectives.

(b) Establish risk appetites for categories such as financial risk, fraud, reputational risk, and cybersecurity, ensuring that decision-making aligns with the Council's strategic objectives. For example, higher risk tolerance may be allowed for innovation-driven projects, while compliance-related risks may have very low tolerance.

(c) The Enterprise Risk Management Committee will review and set risk appetites for each risk on the ERR. This ensures that risk-taking remains within agreed limits and supports effective decision-making.

3.05 Risk Assessment and Classification

Define the level of risk that the City is willing to accept for each risk category, aligning with City Council's strategic objectives by:

(a) Utilize a risk assessment matrix to categorize risks by severity (e.g., low, medium, high).

(b) Conduct qualitative and quantitative risk analysis.

(c) Evaluate the consequences on data confidentiality, residents' safety, legal obligations, and fraud-related impacts (e.g., financial loss, compliance exposure, reputational harm).

(d) Establish a process for prioritizing risks based on their assessed level.

3.06 Risk Mitigation and Control

Provide guidance on how to manage and mitigate identified risks, by:

(a) Defining risk response strategies: avoidance, reduction, sharing, or acceptance.

(b) Implementing control measures such as security protocols, training, fraud prevention and detection controls, and policy updates.

(c) Assigning responsibility for risk management actions to designated departments or individuals.

(d) Establishing timelines for risk mitigation activities and regular progress reviews.

(e) Ensure risk appetite is a guiding factor in the development of mitigation strategies, especially for risks with high potential impact, like cybersecurity breaches or regulatory compliance failures.

3.07 Risk Monitoring and Reporting

Determine how risks will be continuously monitored and reported to ensure they remain under control by:

(a) Implementing a risk monitoring framework with key performance indicators (KPI) and regular reporting cycles (e.g., monthly or quarterly).

(b) Setting up a process for internal evaluations to ensure compliance with established controls.

(c) Creating a system for escalating significant risks to ELT and the Audit Committee, including fraud risks that exceed appetite (recognizing that reporting and investigation of suspected or alleged fraud are governed by the Whistleblower Policy).

(d) Regularly updating the risk register based on new insights and feedback.

3.08 Risk Response

(a) Develop strategies to mitigate, transfer, avoid, or accept risks.

(b) Risk Owners will ensure that appropriate actions are taken based on the risk appetite for their specific area. This can include risk transfer strategies like insurance for high-severity risks or developing internal controls to reduce the likelihood of operational disruptions.

3.09 Incident Response

Define the steps to be taken in response to a risk event or incident by:

(a) Outlining clear protocols for incident reporting and escalation.

(b) Defining roles and responsibilities for the incident response team.

(c) Developing a communication plan for internal and external stakeholders in case of a breach or failure.

(d) Providing guidelines for post-incident evaluation and improvement actions.

3.10 Training and Awareness

Ensuring that all employees are aware of their role in risk management by:

(a) Conducting regular training sessions on risk identification, data security, and CMH-specific protocols, including fraud awareness and reporting.

(b) Maintaining up-to-date resources and materials to support ongoing risk awareness.

(c) Integrating risk management responsibilities into employee performance evaluations where applicable.

3.11 Trending Risks

Stay informed of and respond to the most pressing and prevalent risks affecting similar organizations by:

(a) Maintaining a real-time risk intelligence system by monitoring trending risks across various sectors, particularly healthcare, municipal governance, and IT.

(b) Track key risk indicators (KRIs) to identify trends in areas like data breaches, public health crises, regulatory changes, and supply chain disruptions.

3.12 Business Objectives and Departmental Risk Management

(a) Business Units will integrate risk management into the daily operations of each business unit at CMH, ensuring that risks are identified, assessed, and managed in alignment with departmental and organizational objectives.

(b) Each department should align its risk identification and mitigation techniques with its key objectives, ensuring that potential risks do not hinder their ability to achieve goals.

(c) Regular risk assessments should be conducted by each department to identify risks that could impact operational efficiency, compliance, and the safety of the City’s data or residents’ information.

3.13 Liaising with the Insurance Officer and Risk Management Claims Analyst

(a) Ensure collaboration with the Insurance Claims Officer and the Risk Management Claims Analyst, who handles insurance matters.

(b) The Insurance Officer and Risk Management Claims Analyst will provide input on insurable risks, ensuring that risks requiring transfer (e.g., through insurance policies) are covered. This collaboration guarantees that risks with potential financial or legal impact are managed holistically.

3.14 Enterprise Risks vs. Operational Risks

(a) Distinguish between enterprise-level strategic risks and operational risks and define the role of the ERM Manager in supporting departments with managing both types of risks.

(i) Enterprise Risks: Risks that could affect the entire organization and its long-term objectives, like regulatory changes or major cybersecurity breaches.

(ii) Operational Risks: Risks that primarily affect specific departments but may not impact the entire organization, unless escalated. These risks should be documented in each department's Operational Risk Register.

(b) Collaboration: The ERM Manager and Risk Owners will collaborate on managing risks, ensuring that operational risks are escalated when necessary for inclusion in the Enterprise Risk Register (ERR).

3.15 Significance of Risk Owners

(a) Define the critical role that Risk Owners play in the risk management process and how they contribute to the success of the City’s ERM framework.

(b) Risk Owners are accountable for implementing risk mitigation strategies, continuously monitoring risk levels, and reporting significant changes.

(c) They collaborate closely with the ERM Manager to ensure risks are managed according to the City’s risk appetite and organizational objectives.

(d) Risk Owners also play a key role in ensuring that operational risks are identified, assessed, and escalated when necessary.

3.16 Escalation of Significant Risks

(a) Create a system for escalating significant risks to the Executive Leadership Team (ELT) and the Audit Committee.

(b) Risks that exceed the City’s risk appetite or pose significant threats to strategic objectives will be escalated to the ELT and Audit Committee. Regular reporting will ensure that critical risks are addressed promptly.

3.17 Contractor and Third-Party Risk Management

Outline the process for identifying and managing risks associated with contractors, vendors, and third-party partners that CMH engages with, including those who provide services or products, handle sensitive data, or support operational functions through:

(a) Identification of Third-Party Risks:

(1) Identify critical third parties, including vendors, suppliers, contractors, and service providers, based on their level of involvement with key City operations or systems.

(2) Assess the risks specific to each third party, such as compliance risks (e.g., failure to meet regulatory requirements), cybersecurity risks (e.g., data breaches), financial instability, or performance failures.

(3) Categories of Third-Party Risks: Risks should be categorized based on their potential to disrupt business continuity, such as supply chain risks, reputational risks, and data privacy breaches.

(b) Due Diligence and Vendor Selection:

(1) Conduct thorough due diligence before engaging with third-party contractors. This includes evaluating their financial stability, cybersecurity protocols, compliance with relevant regulations (e.g., HIPAA or data protection laws), and previous performance.

(2) Implement a vendor risk assessment tool to score potential contractors based on factors such as security, financial health, and operational risk.

(3) Require third-party contractors to meet the City's standards for data protection, confidentiality, and quality of service as a part of the procurement and contract negotiation process.

(c) Contractual Safeguards

(1) Develop and include specific contractual provisions that outline the responsibilities and obligations of contractors.

(2) Ensure contracts contain clauses for data protection, confidentiality, audit rights, compliance with regulatory frameworks, and service level agreements (SLAs).

(3) Specify terms for risk mitigation strategies, insurance coverage, and contingency plans in case of contractor default or service disruptions.

(d) Ongoing Monitoring and Compliance

(1) Set up a continuous monitoring framework to track the performance and compliance of contractors and third parties.

(2) Establish regular audit and review processes to ensure that contractors are meeting the required standards, SLAs, and regulatory requirements.

(3) Use key performance indicators (KPIs) and other metrics to measure the success of third-party relationships and identify areas for improvement.

(e) Risk Mitigation Strategies for Third Parties

(1) Develop a risk mitigation plan for contractors, including backup plans for critical service providers or suppliers.

(2) Implement cybersecurity controls, such as data encryption, secure file transfers, and limited access permissions for contractors dealing with sensitive data.

(3) Require third-party contractors to have their own risk management frameworks, including business continuity and disaster recovery plans, to ensure alignment with CMH's risk tolerance.

(f) Contractor Exit Strategy

(1) Define exit strategies in case a contractor is no longer able to meet their obligations or presents too high of a risk.

(2) Include clauses in contracts for smooth termination of agreements and transition plans for services to ensure minimal disruption to the City's operations.

(3) Safeguard against data breaches by ensuring the return or destruction of the City's data when terminating contracts with third parties.

(g) Third-Party Risk Incident Response

(1) Develop an incident response protocol specific to third-party risks, outlining steps to take if a vendor or contractor experiences a data breach, service outage, or fails to meet compliance obligations.

(2) Ensure contractors are contractually obligated to report incidents to CMH immediately and cooperate fully in the investigation and resolution process.

(h) Vendor Risk Register and Reporting

(1) Include identified third-party risks in the City's Enterprise Risk Register (ERR) to ensure a holistic view of all organizational risks.

(2) Establish reporting mechanisms that allow for the periodic evaluation of third-party risks by the executive team and ERM Manager.

3.18 Alignment with City Council's Strategic Objectives

(a) Ensure that the ERM framework supports the Council's long-term strategic objectives.

(b) The ERM Manager will work closely with the ELT and Council to ensure that risk management aligns with strategic priorities, such as growth, regulatory compliance, sustainability, and community trust. By aligning risk management with strategic objectives, CMH ensures that risks are managed in a way that supports the achievement of its broader goals.