Item 13.1.2

AUDITOR GENERAL

Halifax Regional Municipality

Enterprise Risk Management Audit

July 2024

July 12, 2024

The following audit of **Enterprise Risk Management** completed under section 50(2) of the Halifax Regional Municipality Charter, is hereby submitted to the Audit and Finance Standing Committee of Regional Council.

Respectfully,

Original signed by

Andrew Atherton, CPA, CA
Auditor General
Halifax Regional Municipality

AUDITOR GENERAL
Halifax Regional Municipality

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4
www.hrmauditorgeneral.ca
902.490.8407

Table of Contents

Enterprise Risk Management Audit

Risk Management Not Prioritized

Inadequate oversight of both enterprise and operational risk management

- Risk management committee not yet established
- 9 of 11 internal report recommendations not implemented

No risk management training offered

Enterprise Risk Management

Framework exists – requires update and not followed consistently

No policies to support implementation

Operational Risk Management

No process to appropriately manage operational risks

Corporate leadership required to ensure proper risk management at business units

Risks are identified – not well managed

- 4 of 10 enterprise risks have no controls identified
  - Remaining 6 have controls identified but have not been assessed for effectiveness
- Only 6 of 20 operational risks have controls identified, none were assessed for effectiveness
- None of the 30 total risks tested have appropriate treatment plans

Auditor General Halifax Regional Municipality

July 2024

Audit Results

Enterprise Risk is Not Effectively Managed

HRM risk management practices require significant improvement. There is a lack of appropriate oversight over enterprise and operational risk management. It is not sufficient to have an enterprise risk management framework, it is important to ensure the framework is relevant and appropriate risk management practices are communicated and followed. An effective enterprise risk management program requires dedicated commitment from those charged with governance and management to ensure relevant risks are identified and effectively managed across the organization. An effective program will be important as HRM continues to experience significant growth.

Strategic (Enterprise) Risks

• • •

"Risks arising from or related to long-term strategic priorities. These risks must meet one or more of the following criteria: 1: The risk relates directly to one or more of the Priority Outcomes; 2: A risk that has significant impact on multiple operations if realized; 3: There are concerns over the adequacy of Business Unit arrangements for managing a specific risk."

Operational Risks

• • •

"Risks arising from or relating to the execution of day-to-day operations and service delivery."

(Source: HRM's ERM Framework)

Significant gaps in risk management oversight function

According to the Enterprise Risk Management (ERM) Framework, Regional Council through its Audit and Finance Standing Committee (AFSC) is responsible for monitoring and overseeing the adequacy and effectiveness of HRM's risk management framework and risk management plans. However, the ERM status reports presented to the AFSC are not comprehensive enough to communicate most of the gaps in the risk management program. ERM reports were presented once in 2021 and again in 2024, nothing was presented in 2022 and 2023. We expected the issues identified in this audit report to have been discussed with the elected officials through regular updates. However, most of them were not.

Additionally, AFSC is supposed to periodically review the enterprise risk register and challenge the risk management process, but neither has occurred. There is also no process to ensure Management periodically assesses the performance of the entire ERM program and report the result to the AFSC. Comprehensive, accurate and regular reporting of risk management performance contributes to good governance.

We identified concerns with the information included in a risk maturity model assessment performed during the audit period and presented to AFSC in January 2024. We noted some information included in the report that was not consistent with what we found in our audit. Concerns included references that imply strong oversight and management of enterprise risks, and a suggestion that treatment plans were in place. It is important that any information presented to Council, or its committees, be thoroughly validated to ensure it is accurate. There is also a need for AFSC to have sufficient understanding of the existing ERM approach that they can ask the right questions to determine the accuracy of information provided to them.

Legal & Legislative Services' Risk and Insurance division indicated to us that they have recently updated this assessment through surveys completed by the business units, but this is yet to be reported to the AFSC.

Business unit management, as ERM risk owners, have the responsibility to manage risk within their business units and provide assurance on the effectiveness of the internal control environment. However, none of the identified enterprise risks have appropriate risk treatment plans nor have the existing controls been assessed for effectiveness.

Risks Owners

• • •

"Person or entity with the accountability to manage a risk. The person is accountable for the overall management of the risks including bidding for resources to control the risks."

Control Owners

• • •

"Person that has accountability for a task to control an aspect of the risk either the cause or effect. The role is accountable to the Risk Owner."

(Source: HRM's ERM Framework)

The ERM Framework requires the Executive Leadership Team, which includes all business unit executive directors, to meet bi-annually to review the ERM framework, assess the progress of the program against the risk mitigation plan and review enterprise risks over the set tolerance level. However, none of these were done at the meetings held during the audit period. During these meetings, Risk and Insurance provided ERM program status updates and plans, and in April 2024 discussed updates to the ERM process.

In 2021, the Risk and Insurance division was assigned to provide business units and executives with required risk management guidance. We found that the division met with the business units to discuss potential risks and is developing a risk management dashboard that provides a high-level summary of the risk registries. However, Risk and Insurance needs to help ensure relevant parties perform their risk management responsibilities. We expected that the gaps we found in the enterprise risk management process would have been identified and addressed since the

division took over the risk management oversight role over three years ago. Management said the division lacked resources to help with the new risk management responsibility and a risk management staff member was hired in January 2024.

Having a strong organization-wide risk management culture is important to ensure key internal and external uncertainties that could impact achieving regional council and administrative priorities are well managed.

Recommendation 1

Risk and Insurance should implement relevant policies and processes focused on risk management oversight responsibilities to help ensure required tasks are performed by all relevant parties.

Management Response

Agreed. Over the next 12-18 months Risk and Insurance will complete and implement policies and processes which will include oversight responsibilities. Additional administrative support will be hired to support the development of required policies and ongoing operation of newly developed processes. An ERM software solution will be implemented to provide a common tool for risk management consistent monitoring and oversight of risk management information.

Recommendation 2

Risk and Insurance should ensure there is periodic review of the Enterprise Risk Management program, and the result of the assessment is accurately reported to those charged with governance.

Management Response

Agreed. A review of the program and associated reporting into ERM policies and processes will be completed in conjunction with the implementation of the ERM software solution to enable periodic, effective monitoring and review of risk management activities as recommended.

Early in 2023, HRM's Corporate Planning & Performance department conducted a process review of the Enterprise Risk Management program on behalf of Risk and Insurance. The review provided 11 recommendations, out of which two are complete and nine are outstanding. Some of the gaps identified in this audit report were also included in the Corporate Planning & Performance report presented to Risk and Insurance. The report identified five highest priority recommendations, of which four remained outstanding as of May 2024. Those four recommendations suggested that Risk and Insurance should:

- Work with business units to develop risk treatment plans.
- Support business units to identify and assess operational risks.

- Increase knowledge and awareness of ERM process through targeted training.
- Identify and measure outcome-based performance measures.

Failure to implement nine of eleven recommendations demonstrates the lack of emphasis placed on risk management corporately by HRM. Having an effective risk management program should be a corporate goal, but for this to happen, more priority will need to be placed on it.

Key risk management role not in place, key responsibilities not completed

A key risk management committee is yet to be established. The Enterprise Risk Management Framework includes roles and responsibilities for risk management in HRM. However, we found that key parties did not perform their responsibilities.

HRM lacks a risk management committee as defined in its ERM Framework to oversee risk management activities (see sidebar). Establishing this committee was one of the recommendations in the report received from Corporate Planning & Performance that was discussed earlier. Management said the formation of this committee was deferred due to Covid-19, but we expected it to be formed by now. Management indicated they plan to establish the committee by early 2025.

The framework states that risk owners are responsible for overall management of assigned risks and are to provide control owners with risk management tasks. However, none of the risks in the register have an identified control owner. Additionally, existing controls expected to mitigate risks are not assessed for effectiveness and none of the documented mitigating initiatives showed how the risks are being treated. This lack of detail and ownership makes risk monitoring difficult.

Risk Management Committee

• • •

"The Committee supports business units in the identification, assessment, and guidance of risk treatment. The Committee determines if operational or project risk should be escalated to the level of strategic risk for appropriate review and monitoring."

"Annually and as necessary the Risk Management Committee meets to review the Strategic, Operational and Project Risk registers. The committee challenges the identification of risks as well as their assessments. This Committee provides assurance that potential high-level risks are identified and that all risks are rated appropriately to the Senior Leadership Team."

(Source: HRM's ERM Framework)

We interviewed four members of HRM executive management responsible for managing the enterprise risks we tested to see if they understood their responsibilities as risk owners. Three of the four said their responsibilities were not communicated. One of the three said the risk

management responsibilities are understood, but it is unclear in the framework which aspects they are responsible for. All four said the risk-related meetings held with Risk and Insurance focused on identifying potential risks in their business units and reviewing risk ratings, but do not cover any additional responsibilities related to managing or mitigating existing risks.

Nine out of ten business unit coordinators we interviewed either said they do not use the framework, or they were not aware it existed. Risk and Insurance management told us they did not circulate the ERM Framework because it was established before they took over enterprise risk management and expected the business units to already have the framework.

We found it is often not clear who should be responsible for a risk management process; for example, the framework does not clearly state who should determine the existing controls that mitigate the risks and assess their effectiveness. It states enterprise risks should be reviewed based on the significance of the risk, but it does not say who is responsible.

It is important that all key risk management roles are clearly established, responsibilities include relevant details, and these are communicated to necessary parties. This should help ensure relevant risk management practices are consistently and effectively performed.

Recommendation 3

Risk and Insurance should ensure key roles and responsibilities are established, clearly defined, and communicated to all parties involved in the risk management process.

Management Response

Agreed. With the separation of the ERM policy from the framework, clarity of roles and responsibilities within policies and processes will be better defined over the next 12-18 months. Risk and Insurance will support business units to ensure they have the awareness, knowledge, tools, and resources required to carry out their required ERM duties.

Enterprise Risk Management Framework requires update

HRM's Enterprise Risk Management Framework was developed in 2019 to provide guidance for risk management practices. However, we identified some concerns in the framework. We expected the framework to be reviewed periodically and updated as necessary when there is a new version of the risk management guideline available. However, no significant review has been done since the framework was developed. Management told us there are plans to review and update the Enterprise Risk Management Framework but there is no documented timeline for when that will be done.

Some of the concerns identified in the framework include:

- Risk management scope not appropriately defined – Risk and Insurance management told us the framework does not apply to operational risks even though it is specifically noted in the document.
- Risk treatment plan components not included.
- Residual risk determination not included.
- No clear link to business and strategic priority planning process.

For effective risk management, it is important to have a clear and relevant risk management framework that will provide an appropriate and consistent organization-wide risk management approach.

Recommendation 4

Risk and Insurance should review the current risk management framework, make relevant updates, and determine a schedule for periodic subsequent reviews.

Management Response

Agreed. Risk and Insurance will additionally integrate periodic framework review and associated reporting on ERM policies and processes. This review is to be completed along with updates to the Strategic Plan. This will be accomplished through collaborating with Strategic Planning & Performance to include risk consideration with Strategic Planning Process, coordinating with Risk Owners to capture risks which may prevent achievement of goals in new strategic plan and risks which arise from pursuing goals in strategic plan, meeting with Risk Owners to capture updates to Strategic Risk Register semi-annually.

Lack of clear guidance for risk management activities

HRM lacks policies and procedures to provide guidance for risk management practices. These are required to provide detailed guidance on how to implement ERM practices outlined in the framework. The risk evaluation, treatment, monitoring, and reporting sections of the framework do not provide sufficient details on how and when each activity should be performed. The framework also has no guidance on how residual risk should be determined to help make informed risk management decisions. It defines responsibilities at a high level and does not provide details of all key responsibilities expected from each party. Having detailed procedures to support the framework will help provide clarity on responsibilities.

Corporate Planning & Performance reports the percentage of risks above the established tolerance level, but the reporting section in the framework has no information on what enterprise risk performance measures will be reported, by whom, and in what form.

Procedures that provide relevant guidance on how the policies in the risk management framework should be implemented would provide clarity on responsibilities. This would also help prevent knowledge loss when there is employee turnover in the organization.

Recommendation 5

Risk and Insurance should develop risk management policies and procedures to support the ERM Framework and provide guidance on risk management practices across HRM.

Management Response

Agreed. Risk and Insurance will undertake this work over the next 12 to 18 months as part of the initiation and preparation for roll out of ERM practices.

Enterprise Risk Management Practices Not Consistently Followed

We compared HRM's current risk management practices with the Enterprise Risk Management Framework and the recognized risk management guidelines which outline effective risk management processes. We found HRM enterprise risk management processes are not consistent with key aspects of the guidelines or their own framework.

Appropriate risk assessment practices not consistently followed

HRM has no process to ensure regional council and administrative priorities are considered before risks are identified. Enterprise risks are currently linked to the applicable priority area after the risk has been identified. The framework does not include a process to consider these priority areas during risk identification. The purpose of risk identification is to define the risks that may impact the organization's ability to achieve its objectives. Understanding HRM's priority areas will help ensure risk factors that impact them are considered and addressed.

HRM does not follow the risk identification steps outlined in its Enterprise Risk Management Framework. The internal and external factors of the organization are supposed to be assessed using a strength, weakness, opportunity, and threat (SWOT) methodology, with the result updated annually. However, SWOTs were only drafted in 2018 and 2022 but neither were finalized. Instead, we found the Risk and Insurance division met annually with the business units to discuss potential risks. In addition, in 2022 and 2023, the division developed and sent surveys to all business units to identify factors that affect the organization and potential risks affecting their units. These are good first steps. However, HRM needs a structured and effective risk identification process.

Recommendation 6

Risk and Insurance should ensure an appropriate risk identification process is incorporated in the risk management framework.

Management Response

Agreed. Risk and Insurance has initiated a process to review risks that have been previously identified and we will ensure the new processes are reflected in updates made to the framework. Discussions will be held with Risk Owners to ensure that they are appropriately supported in the identification of enterprise risks. In addition, a new Risk Analyst resource will be hired to support the Operational Risk Management Program. The ERM software solution will be implemented to enable centralized collection of newly identified risks and provide period reports on their status to ELT and the various Risk Owners.

Lack of appropriate and detailed risk treatment plans

We reviewed ten enterprise risks from HRM's risk register and found gaps in managing all ten. We expect risk owners to be responsible for evaluating the effectiveness of existing internal controls that would mitigate identified risks. For four of the risks reviewed, we found internal controls to mitigate the risks were not documented. For the remaining six, while internal controls were identified, none were assessed for effectiveness. Documenting controls that mitigate identified risk and assessing their effectiveness is important to help assess the level of risks the organization is exposed to and to guide development of appropriate risk treatment approach and plans.

Recommendation 7

Risk and Insurance should work with all business units to ensure relevant, existing controls are documented and assessed for effectiveness.

Management Response

Agreed. Risk and Insurance will work with Business Units to capture risk control information to demonstrate that relevant risk controls have been identified, documented, and assessed.

HRM does not have documented risk treatment plans that demonstrate how enterprise risks are being managed and it is unclear what risk treatment approaches were chosen. All ten enterprise risks we reviewed did not have comprehensive risk treatment plans and the decision to transfer, avoid, or accept is not documented for any of the risks. The risk management guidelines outline relevant information expected in a treatment plan. Two of the seven components are partially addressed in the risk register, but the following five were not addressed at all:

- Rationale for selecting the treatment option and benefits expected,
- Identifying those accountable for approving and implementing the plan,
- Resources required and contingencies,
- Performance measures and constraints, and
- Reporting and monitoring requirements.

For nine of the ten risks reviewed, the HRM risk register includes initiatives and deliverables with timelines identified for business and budget planning purposes, which may address some of the risks. However, it is not clear how the specific deliverables will address the risks or at what point individual risks would be reduced to a tolerable level. Business unit management told us they believe the sampled risks are being mitigated, but this is not tracked. One of the ten had no documented initiatives or deliverables. We expected each enterprise risk to have a documented list of relevant actions or initiatives that help to mitigate them including an explanation of how each action will reduce the risk in question. Each risk should then have a summary showing the risk remaining (residual risk) after the various actions are taken.

We found no one is assessing the impact of these actions on enterprise risks. For all ten risks, what amount of the risk yet to be treated, is not known. Risk and Insurance introduced the residual rating concept for business units to determine what the risk impact and likelihood ratings will be after treatment. However, ratings are not useful without details of what risk is remaining. It is important to periodically assess and document risks remaining after treatment to ensure appropriate mitigation plans are further developed, as necessary.

In addition, the enterprise risk register does not include all relevant risk management sections. For example, there is no section for gross (without existing controls) risk, comprehensive treatment plan, residual risk description and control assessment result. Having these important sections will help to ensure risks are appropriately managed.

Testing Results – Enterprise Risk Management Process

Enterprise Risk Management Process Steps	# of Risks Tested that Complied
Existing controls identified	6/10
Effectiveness of existing controls assessed	0/6
Clear risk approach	0/10
Gross risk rating	0/10
Net risk rating	10/10
Residual risk assessed and documented	0/10
Appropriate risk treatment plans	0/10
Risk owners assigned	10/10
Control owners assigned	0/10
Periodic review done based on risk type	0/10

Recommendation 8

Risk and Insurance should work with all business units to develop appropriate structured risk treatment plans and ensure risks remaining after treatment are periodically assessed and documented. Clear treatment approach should also be documented, and the risk register updated accordingly.

Management Response

Agreed. Risk and Insurance will work with Business Units during the implementation of their operational risk registries to capture, for both operational and relevant enterprise risks, their risk treatment plans and residual risk information. This will demonstrate that relevant risk treatments have been developed, documented, and assessed and that residual risk is assessed and documented.

Gaps in enterprise risk performance measurement

HRM has set a risk tolerance level and the percentage of enterprise risk above the tolerance level was reported in HRM's strategic priority report during the audit period. However, no documented action was taken on how risks in that category are reduced or mitigated.

The framework includes monitoring requirements for different categories of risks, requiring significant risks be reviewed quarterly, but this is not done.

It is important to review the performance of enterprise risk management, including significant risks, to assess if the program objectives are met and to ensure significant risks are appropriately managed.

Recommendation 9

Risk and Insurance should ensure there is a documented process to measure enterprise risk management performance, including having specific monitoring and reporting plans for significant risks.

Management Response

Agreed. An ERM software solution will be implemented to enable centralized collection of identified risks and provide periodic reports on their status to ELT and the various Risk Owners. Individual Risk Owners or Risk Controllers will be required, with guidance from Risk and Insurance, to update the system to track risk treatment, risk controls and residual risks. This will enable appropriate reporting and escalation as may be appropriate.

Significant Gaps in Operational Risk Management

HRM has no consistent process to appropriately manage its operational risks. We sampled 20 operational risks identified in the registers and checked if the process followed recognized risk management guidelines. We found significant gaps in the process. Some risks had no risk owners assigned to manage them. None of the 20 sampled risks had documented treatment plans that demonstrate how the operational risks are being mitigated. The Planning & Development business unit did not maintain an operational risk register, others have registers, but these require significant improvement. Management needs to formally monitor operational risks to ensure key concerns that could impact business operations are identified and appropriately managed.

Poor and inconsistent processes for operational risk management

We found gaps in operational risk management similar to those noted in the enterprise risk assessment and treatment sections of this report. There needs to be a consistent approach for risk identification. We found only the Property, Fleet and Environment business unit performed a SWOT analysis in addition to having meetings to assess internal and external factors that affect the unit. They also maintained better operational risk management records than others. Other business units said they do meet to discuss potential risks but only three of nine business units we tested could provide some evidence of this.

For all 20 operational risks tested, what aspect of the risk yet to be treated is not known. Controls that mitigate the risks are not determined in most cases, and where done, the effectiveness of these controls is not assessed. Similarly, none of the operational risks we tested have risk treatment plans. In most cases, the register includes completed and planned deliverables. However, the register does not include timelines for these planned deliverables and the overall treatment strategy to mitigate each risk is not documented. Just like enterprise risk, relevant information required by the risk management guidelines for a risk treatment plan is lacking. Management said there are initiatives and deliverables identified during the business planning process that would mitigate each risk. However, the lack of a coordinated risk management approach makes knowing the impact of these initiatives difficult to determine.

Having a standardized and consistent process should help ensure risks that affect HRM's day-to-day operations are appropriately managed.

Testing Results – Operational Risk Management Process

Operational Risk Management Process Steps	# of Risks Tested that Complied
Existing controls identified	6/20
Effectiveness of existing controls assessed	0/6
Clear risk approach	0/20
Appropriate risk treatment plans	0/20
Residual risk assessed and documented	0/20
Risk owners assigned	12/20

Recommendation 10

HRM should ensure there is a standardized and consistent operational risk management process to ensure risks are appropriately identified and managed.

Management Response

Agreed. Operational risk management has not been previously corporately adopted by HRM. Risk and Insurance will develop ERM policies and processes to support standardized and consistent operational risk management practices. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program.

Lack of oversight over operational risk management

The CAO told us her office has overall responsibility for operational risk management, but she also noted that this was an area where a more developed and consistent approach was needed. She identified that there are no standardized and consistent processes for operational risk management within business units, but she will make this a priority and use the lessons from this audit going forward. We found and noted earlier in this report that a Risk Management Committee expected to have oversight responsibilities over business unit operational risk has not been established. The ERM Framework includes operational risk management and the most recent job descriptions for Risk and Insurance's Chief Risk Officer and Enterprise Risk & Insurance Analyst state that they are responsible for it. However, Risk and Insurance management told us that they are not responsible for operational risk management.

Business unit management told us they have informal periodic meetings with risk owners and business unit coordinators and make updates as necessary to the registers. No support was provided for the meetings in most cases and in some cases no dates are listed in the register to see when updates were made. The current operational risk registers also lack key sections to help effectively manage operational risks.

Two of the business units asked our auditors for copies of their own registers during the audit. We also found that three key operational risks were documented as transferred in the operational risk registers of the individual business units. However, the risks were not found in the registers of the business unit the risk was supposed to have been transferred to. It is important that the risk management process and its outcomes are consistently documented and retained where accessible to relevant staff.

There are no reports to Regional Council's AFSC on operational risk management. Additionally, there is no evidence that operational risks are monitored by the CAO's Office. The CAO told us that operational risks are often discussed during the weekly meetings held with the Executive Leadership Team but there are no minutes for these meetings.

Gaps identified in operational risk assessment and treatment processes makes it difficult for management to effectively manage the risks.

Recommendation 11

HRM should ensure the risk management processes include a requirement to monitor and report operational risks by all relevant parties.

Management Response

Agreed. Operational risk management monitoring and reporting will be required, reporting and monitoring requirements will be outlined in risk management policies and processes. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program. An ERM software solution will be implemented to enable effective documentation, monitoring, updating, and reporting of risks.

Recommendation 12

HRM should ensure appropriate documentation and records are maintained for key operational risk management practices.

Management Response

Agreed. Documentation and records management will be integrated into risk management policies and processes. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program. An ERM software solution will be implemented to enable effective documentation, monitoring, updating, and reporting of risks. Additional administrative support will be hired in order to support the development of operational risk management policies and the ongoing operation of new processes.

No Risk Management Training

HRM does not offer risk management training within the organization. Risk management guidelines recommend that organizations conduct training so that those responsible for risk management will understand their roles, but no training was offered during the audit period.

Business unit coordinators are responsible for promoting risk management in their unit and to provide guidance on risk application to risk owners. However, four of the ten business unit coordinators we interviewed said they have not attended any relevant training, the remaining six told us they attended five years ago. Periodic risk management training would help ensure a risk management awareness culture is cultivated within the organization.

In addition, no training has been held for elected officials. HRM's Audit and Finance Standing Committee has oversight responsibility for risk management and members should be offered training to better understand this role.

Risk and Insurance is drafting a risk management introductory training module for employees, which may be helpful for elected officials as well. Training programs will assist all parties to understand and perform their responsibilities appropriately.

Recommendation 13

Risk and Insurance should develop an appropriate training program for the organization.

Management Response

Agreed. This is in progress. Risk and Insurance had initiated the development of a training module to support and enable delivery of Enterprise Risk Management across the organization prior to this audit, and the findings from this audit will be taken into consideration when finalizing the training program.

Recommendation 14

Risk and Insurance should ensure risk management training is periodically offered to all HRM employees and elected officials. The training should be mandatory for all parties performing key risk management responsibilities.

Management Response

Agreed. This will be addressed as part of the training noted in response to Recommendation 13.

Background

The Risk and Insurance Services Division of the Legal & Legislative Services business unit is responsible for Enterprise Risk Management (ERM) in HRM. According to the HRM 2023-24 business plan, this includes "*ensuring that risks (strategic and operational) are appropriately identified through the business planning process, evaluated, and managed by the responsible business units*."

Enterprise risk management *is an "organizational-wide approach to identify, prioritize, and manage potential risks and opportunities." (Source: HRM's ERM Framework).* HRM's Enterprise Risk Management Framework says that it provides systemic guidance on risk management to all business units and that it is based on internationally recognized risk management guidelines, Canada Standards Association, CSA ISO 31000:2009.

Administrative Order One (The Procedure Of The Council Administrative Order), Schedule 2, section 4 defines the responsibility of the Audit and Finance Standing Committee in relation to risk management to include *"(d) ensuring the adequacy and effectiveness of the systems of internal control in relation to financial controls and risk management as established by Administration;* and *(e) reviewing bi-annually with management, the enterprise risk management and financial implications coming from such risk and implications, including: Environmental, Human Resources, Operational and the insurable risks and insurance coverage strategy of the Municipality*".

Operational risks are defined according to the HRM ERM framework as *"risks arising from or relating to the execution of day-to-day operations and service delivery."* These are managed by individual business units. The Chief Administrative Officer has overall accountability for risk management in HRM.

About the Audit

We completed a performance audit of Enterprise Risk Management. Our role is to express an independent audit opinion of this area.

The objectives of the audit were:

- To determine if HRM has an appropriate Enterprise Risk Management program that helps identify and manage key organizational risks; and
- To determine whether HRM has appropriate operational risk management processes that help identify and manage key operational risks.

We developed the criteria for this audit. These were discussed with, and accepted as appropriate by, management of Legal & Legislative Services, Finance & Asset Management and Chief Administrative Office.

1. Enterprise risk management policies and procedures should be documented and consistent with risk management principles and guidelines.
2. Roles and responsibilities should be established and clearly defined.
3. Enterprise risk management processes should ensure key risks to achieving regional council and administrative priorities are identified, documented, communicated, and monitored.
4. Performance of the risk management program should be periodically evaluated and reported.
5. HRM's employees and those responsible for ERM governance should be provided with risk management awareness training.
6. Operational risks should be identified, documented, communicated, and monitored.
7. Operational risk management processes should be consistent with relevant policies and standards.
8. HRM senior management should oversee operational risk management activities to ensure key risks are identified and managed and elevate risks to the enterprise level as appropriate.

Our audit period was April 1, 2021 – September 30, 2023. Information from outside the audit period was considered, as necessary.

Our audit approach included: interviews with management and staff in Legal & Legislative Services, Finance & Asset Management, and other business units as necessary; examination and review of relevant documentation supporting the subject matter; and review of internal policies, procedures, and programs.

This audit was conducted in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001 Direct Engagements published by the Chartered Professional Accountants of Canada.

We apply CPA Canada's Canadian Standard on Quality Management 1. Our staff comply with the independence and ethical requirements of the Chartered Professional Accountants of Nova Scotia Code of Conduct.

Appendix 1 – Recommendations and Management Responses

Recommendation 1

Risk and Insurance should implement relevant policies and processes focused on risk management oversight responsibilities to help ensure required tasks are performed by all relevant parties.

Management Response

Agreed. Over the next 12-18 months Risk and Insurance will complete and implement policies and processes which will include oversight responsibilities. Additional administrative support will be hired to support the development of required policies and ongoing operation of newly developed processes. An ERM software solution will be implemented to provide a common tool for risk management consistent monitoring and oversight of risk management information.

Recommendation 2

Risk and Insurance should ensure there is periodic review of the Enterprise Risk Management program, and the result of the assessment is accurately reported to those charged with governance.

Management Response

Agreed. A review of the program and associated reporting into ERM policies and processes will be completed in conjunction with the implementation of the ERM software solution to enable periodic, effective monitoring and review of risk management activities as recommended.

Recommendation 3

Risk and Insurance should ensure key roles and responsibilities are established, clearly defined, and communicated to all parties involved in the risk management process.

Management Response

Agreed. With the separation of the ERM policy from the framework, clarity of roles and responsibilities within policies and processes will be better defined over the next 12-18 months. Risk and Insurance will support business units to ensure they have the awareness, knowledge, tools, and resources required to carry out their required ERM duties.

Recommendation 4

Risk and Insurance should review the current risk management framework, make relevant updates, and determine a schedule for periodic subsequent reviews.

Management Response

Agreed. Risk and Insurance will additionally integrate periodic framework review and associated reporting on ERM policies and processes. This review is to be completed along with updates to the Strategic Plan. This will be accomplished through collaborating with Strategic Planning & Performance to include risk consideration with Strategic Planning Process, coordinating with Risk Owners to capture risks which may prevent achievement of goals in new strategic plan and risks which arise from pursuing goals in strategic plan, meeting with Risk Owners to capture updates to Strategic Risk Register semi-annually.

Recommendation 5

Risk and Insurance should develop risk management policies and procedures to support the ERM Framework and provide guidance on risk management practices across HRM.

Management Response

Agreed. Risk and Insurance will undertake this work over the next 12 to 18 months as part of the initiation and preparation for roll out of ERM practices.

Recommendation 6

Risk and Insurance should ensure an appropriate risk identification process is incorporated in the risk management framework.

Management Response

Agreed. Risk and Insurance has initiated a process to review risks that have been previously identified and we will ensure the new processes are reflected in updates made to the framework. Discussions will be held with Risk Owners to ensure that they are appropriately supported in the identification of enterprise risks. In addition, a new Risk Analyst resource will be hired to support the Operational Risk Management Program. The ERM software solution will be implemented to enable centralized collection of newly identified risks and provide period reports on their status to ELT and the various Risk Owners.

Recommendation 7

Risk and Insurance should work with all business units to ensure relevant, existing controls are documented and assessed for effectiveness.

Management Response

Agreed. Risk and Insurance will work with Business Units to capture risk control information to demonstrate that relevant risk controls have been identified, documented, and assessed.

Recommendation 8

Risk and Insurance should work with all business units to develop appropriate structured risk treatment plans and ensure risks remaining after treatment are periodically assessed and documented. Clear treatment approach should also be documented, and the risk register updated accordingly.

Management Response

Agreed. Risk and Insurance will work with Business Units during the implementation of their operational risk registries to capture, for both operational and relevant enterprise risks, their risk treatment plans and residual risk information. This will demonstrate that relevant risk treatments have been developed, documented, and assessed and that residual risk is assessed and documented.

Recommendation 9

Risk and Insurance should ensure there is a documented process to measure enterprise risk management performance, including having specific monitoring and reporting plans for significant risks.

Management Response

Agreed. An ERM software solution will be implemented to enable centralized collection of identified risks and provide periodic reports on their status to ELT and the various Risk Owners. Individual Risk Owners or Risk Controllers will be required, with guidance from Risk and Insurance, to update the system to track risk treatment, risk controls and residual risks. This will enable appropriate reporting and escalation as may be appropriate.

Recommendation 10

HRM should ensure there is a standardized and consistent operational risk management process to ensure risks are appropriately identified and managed.

Management Response

Agreed. Operational risk management has not been previously corporately adopted by HRM. Risk and Insurance will develop ERM policies and processes to support standardized and consistent operational risk management practices. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program.

Recommendation 11

HRM should ensure the risk management processes include a requirement to monitor and report operational risks by all relevant parties.

Management Response

Agreed. Operational risk management monitoring and reporting will be required, reporting and monitoring requirements will be outlined in risk management policies and processes. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program. An ERM software solution will be implemented to enable effective documentation, monitoring, updating, and reporting of risks.

Recommendation 12

HRM should ensure appropriate documentation and records are maintained for key operational risk management practices.

Management Response

Agreed. Documentation and records management will be integrated into risk management policies and processes. To ensure Business Units are appropriately supported, an additional Risk Analyst resource will be hired to support the Operational Risk Management Program. An ERM software solution will be implemented to enable effective documentation, monitoring, updating, and reporting of risks. Additional administrative support will be hired in order to support the development of operational risk management policies and the ongoing operation of new processes.

Recommendation 13

Risk and Insurance should develop an appropriate training program for the organization.

Management Response

Agreed. This is in progress. Risk and Insurance had initiated the development of a training module to support and enable delivery of Enterprise Risk Management across the organization prior to this audit, and the findings from this audit will be taken into consideration when finalizing the training program.

Recommendation 14

Risk and Insurance should ensure risk management training is periodically offered to all HRM employees and elected officials. The training should be mandatory for all parties performing key risk management responsibilities.

Management Response

Agreed. This will be addressed as part of the training noted in response to Recommendation 13.

Contact Information

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4

Phone: 902 490 8407
Email: auditorgeneral@halifax.ca
Website: www.hrmauditorgeneral.ca
X: @Halifax AG