



P.O. Box 1749
Halifax, Nova Scotia
B3J 3A5 Canada

Item No. 3
Audit & Finance Standing Committee
January 17, 2024

TO: Mayor Savage and Members of Halifax Regional Council

-ORIGINAL SIGNED-

SUBMITTED BY:

Cathie O'Toole, Chief Administrative Officer

DATE: December 12, 2023

SUBJECT: Enterprise Risk Management Update – November 2023

INFORMATION REPORT

ORIGIN

Following the most recent report to the Committee oversight for Enterprise Risk Management was transferred to Risk and Insurance Services. This report provides an update on the status of the program.

LEGISLATIVE AUTHORITY

Administrative Order One – The Procedures of the Council Administrative Order (AO-01)

Schedule 2 of AO-01 is the Terms of Reference for the Audit and Finance Standing Committee.

1 (1) The purpose of the Audit and Finance Standing Committee is to provide advice to the Council on matters relating to audit and finance.

(2) The other purposes of the Committee are to:

- (a) fulfill the requirements as outlined in Section 48 of the HRM Charter; and
- (b) assist the Council in meeting its responsibilities by ensuring the adequacy and effectiveness of financial reporting, risk management and internal controls.

4. The Audit and Finance Standing Committee shall:

- (d) ensure the adequacy and effectiveness of the systems of internal control in relation to financial controls and risk management as established by Administration;
- (e) review bi-annually with management the enterprise risk management and financial implications coming from such risk and implication's including Environmental, Human Resources, Operational and the insurable risks and insurance coverage strategy of the municipality.

BACKGROUND

At the September 16, 2020, update to Audit and Finance Standing Committee <https://www.halifax.ca/sites/default/files/documents/city-hall/standing-committees/200916afscinfo2.pdf>, HRM's Enterprise Risk Management Strategy was replaced by the adoption of an Enterprise Risk

Management (ERM) Framework; this document details HRM's ERM practice, governance structure and procedures with respect to the management and oversight of risk for the organization.

Pursuant to the Terms of Reference of the Audit and Finance Committee an update on the status of HRM's ERM program is being provided.

DISCUSSION

HRM's Enterprise Risk Management Program was established using the guiding principles of the ISO 31000 Standard on Enterprise Risk Management (ERM). The provisions of this standard require continuous monitoring of both the internal and external environments so that the framework on which the program is established remains both relative and adaptive to the environment in which it operates.

Updates Fiscal 2023 - 2024:

Core Process Review

Upon receipt of the ERM program a process review was completed through Corporate Planning to identify any improvements to the processes of the program. Through this review improvement opportunities were identified, the majority of which had been previously identified by Risk and Insurance Services. The top 5 opportunities are:

1. Implement SharePoint or a similar web-based collaborative platform to store and exchange process data and information with Business Units.
2. Risk Analyst attends and supports Business Unit meetings where they identify and assess new and existing operational risks.
3. Risk Analyst works with Business Units to assist in the development of Risk Treatment Plans.
4. Increase knowledge and awareness of ERM process among key stakeholders and across the organization through targeted training initiatives.
5. Identify and measure outcome-based performance measures that monitor the effectiveness and efficiency of the ERM program and risk treatment plans.

Currently, Risk and Insurance has implemented the use of a SharePoint system that allows Risk Owners to update the status of their risk ratings and mitigation efforts in real time. The remaining recommendations are currently being reviewed and are anticipated to be implemented by Q4 of fiscal 2023 2024. This will be facilitated through the addition of a new Risk Analyst position that will focus on the ERM program.

Council Report Comments

It has been noted that the risk section of Council reports may not have been completed in the manner that was initially anticipated. A new set of guidelines were created and implemented to provide report writers with direction on when to complete a risk and the different types of risks that exists. The methodology behind the content came from interviews with report writers to garner a better understanding of their process, concerns, and recommendations.

Risk Register

Risk and Insurance has met with Business Units who have been identified as being risk owners to update the rankings of their enterprise risks, explore any new or emerging risk and introducing the concept of net residual risk. Net residual risk is the rating of an enterprise risk that would remain once all mitigating activities have been implemented.

Due to the nature of the risk, it may not be possible for HRM to reduce the likelihood and impact within our tolerance of 3:3 (Likelihood and Impact). Through this process HRM can note and monitor those risks that are and may remain beyond our control but note that they are still being managed

Maturity Model

Risk and Insurance has also reviewed the current Enterprise Risk Management and traditional Risk Management processes and completed an assessment through an industry recognized Risk Maturity Model (Attachment A). Through this analysis insight was gained on how our total Risk Management processes measured against an industry standard. The parameters of the Risk Maturity Model were based on an assessment by Risk staff as to the status on the implementation of risk programs throughout the municipality. The next step will be to provide the Executive Leadership Team with the survey questions so that an updated scoring can be achieved that reflects the opinions of the executive leadership. Once completed the process will be repeated on a bi-annual basis through the Risk Committee, once formed.

Staff Training

A training module designed to inform new hires and existing staff about risk management and the ERM program is currently in development through Risk & Insurance. Working closely with Learning & Development, the intention is that the introductory training module will be rolled out and available for all staff to receive online. This will allow staff to receive the training and build awareness on ERM at an introductory level. In the future, further training can be developed to further enhance HRM's risk culture. It is anticipated that it will be available in fiscal 2024 – 2025.

FINANCIAL IMPLICATIONS

There are no direct financial implications of this report, however heightened attention to risk is a mitigating factor in the reduction of risk (financial, reputational etc.) for the organization.

COMMUNITY ENGAGEMENT

There was no community engagement required for the preparation of this report.

ATTACHMENTS

Attachment A – Risk Maturity Model

A copy of this report can be obtained online at halifax.ca or by contacting the Office of the Municipal Clerk at 902.490.4210.

Report Prepared by: Joel Plater Chief Risk Officer – Manager Risk & Insurance Services 902-222-7230

[Go to survey](#)

RIMS Risk Maturity Model®

Result for: Halifax Regional Municipality

Respondent: Michelle Briar

Date: 2022-05-06 16:53:20

The Benefits of RIMS Membership

RIMS members get access to the tools, thought leadership, and networking opportunities to help you succeed.

Learn more about our global community of risk professionals at www.rims.org.

WHILE THE INFORMATION CONTAINED HEREIN IS BASED ON SOURCES BELIEVED TO BE RELIABLE, RIMS MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESSED OR IMPLIED, REGARDING THE MATERIALS. THE MATERIALS PROVIDE GENERAL GUIDANCE ON SUBJECTS COVERED BY KNOWLEDGEABLE RISK LEADERS, BUT ARE NOT INTENDED TO BE TAKEN AS ADVICE REGARDING ANY PARTICULAR SITUATION. INDIVIDUALS SHOULD CONSULT THEIR ADVISORS REGARDING SPECIFIC RISK MANAGEMENT ISSUES.

TERMS OF USE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THESE MATERIALS (AS THAT TERMS IS DEFINED BELOW). IF YOU DOWNLOAD, ACCESS AND/OR USE ANY OF THESE MATERIALS, YOU ARE AGREEING AND CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT").






The Materials provided to you are NOT for sale and are not being sold to you. You may NOT transfer these materials to any other person or permit any other person to use these Materials. You may only acquire a license to use these Materials and only upon the terms and conditions set forth in this Agreement. Read this Agreement carefully before using these Materials. Do not use these Materials unless you agree with all terms of this Agreement.

1. **License Grant.** Upon your acceptance of the terms of this Agreement in the manner set forth above, the Risk and Insurance Management Society, Inc ("Licensor" or "RIMS") hereby grants to you a nonexclusive, revocable, non-transferable, non-sublicensable, limited license to use the Materials solely for your participation in the related Course and/or for your studies related to the subject matter covered by the relevant examination (if applicable). If applicable, you may download the Materials onto a single device; you may download the Materials onto a second device so long as the first device and second device are not used simultaneously. You are not permitted to lease, rent, distribute or sublicense the Materials or any rights therein. You agree that you have no right, power or authority to make any modifications to or unauthorized copies of the Materials. You agree not to transfer or assign the Materials and/or this Agreement to another party without the prior written consent of Licensor. If such consent is given and you transfer or assign the Materials and/or this Agreement, then you must at the same time either transfer any copies of the Materials to the same party or destroy or return to Licensor any such Materials not transferred. Except as set forth above, you may not transfer or assign the Materials or rights under this Agreement. You agree not to modify, translate, reverse engineer, decompile, disassemble, or create derivative works of the Material or assist someone in performing such prohibited acts.
2. **Materials.** As used in this Agreement, the term "Materials" means and includes any electronic or printed materials provided to you by RIMS, and/or to which you are granted access by RIMS (directly or indirectly) in connection with your license of the Materials and/or the Course, and shall include notes taken by you (by hand, electronically, digitally, or otherwise) while using the Materials; any and all electronically-stored/ accessed/delivered, and/or digitally-stored/accessed/delivered materials included under this License via download to a computer or via access to a web application, and/or otherwise provided to you and/or to which you are otherwise granted access by RIMS (directly or indirectly), including, but not limited to, applications downloadable from a third party in connection with your license of the Materials.
3. **Title.** You agree that Licensor owns and holds title to the Materials and all subsequent copies thereof regardless of the form or media. Furthermore, title, ownership rights, and intellectual property rights in the Materials shall remain with Licensor. The Materials are protected by copyright and other intellectual property laws and by international treaties.
4. **Term and Termination.** This license granted under this Agreement begins on the date you receive the Materials and ends 24 months after that date. You may terminate this license at any time by destroying the Materials and any related documentation together with all copies and merged portions in any form. Your license for the Materials will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination, you agree to destroy the Materials and related documentation, together with all copies thereof. You agree that you will not be entitled to a refund of any applicable license fee upon early termination of this Agreement.
5. **Governing Law.** The laws of the State of New York shall govern the construction of this Agreement and you agree to be subject to personal jurisdiction in the State of New York for the purposes of enforcing the provisions of this Agreement.
6. **No Warranties.** LICENSOR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT OF THIRD PARTIES' RIGHTS. THE MATERIALS ARE PROVIDED TO YOU ON AN "AS IS" BASIS. TO THE FULL EXTENT PERMITTED BY LAW, THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE ABOVE LIMITED WARRANTY PERIOD. MOREOVER, IN NO EVENT WILL WARRANTIES PROVIDED BY LAW, IF ANY, APPLY UNLESS THEY ARE REQUIRED TO APPLY BY STATUTE NOTWITHSTANDING THEIR EXCLUSION BY CONTRACT. NO DEALER, AGENT, OR EMPLOYEE OF LICENSOR IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS LIMITED WARRANTY. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.
7. **Limitation of Remedies.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY SHALL LICENSOR OR ITS SUPPLIERS OR RESELLERS, BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, BUSINESS INTERRUPTIONS, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER PERSONAL OR COMMERCIAL DAMAGES OR LOSSES ARISING FROM THE USE OR INABILITY TO USE THE MATERIALS (WHETHER OR NOT DUE TO ANY DEFECTS THEREIN). IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES EVEN IF LICENSOR SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES OR SUCH DAMAGES WERE REASONABLY FORSEEABLE, OR FOR ANY CLAIM BY ANY OTHER PARTY. IN NO EVENT SHALL LICENSOR'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR THE COURSE FOR WHICH THE MATERIALS ARE PROVIDED.
8. **Indemnification.** You agree to defend, indemnify and hold harmless Licensor, its suppliers and its resellers from and against liabilities, costs, damages and expenses (including settlement costs and reasonable attorneys' fees) arising from any claims from anybody that result from or relate to your use, reproduction or distribution of the Materials.
9. **Severability.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired.

10. **Entire Agreement.** You further agree that this Agreement is the complete and exclusive statement of the agreement between you and Licensor which supersedes all proposals or prior agreements, oral or written, and all other communications between you and Licensor relating to the subject matter of this agreement. This Agreement may only be modified by a written agreement signed by both you and an authorized representative of Licensor.
11. **Acknowledgement.** By downloading, installing or using any part of the Materials, you indicate that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.
12. **Force Majeure.** Licensor shall not be liable hereunder for any failure or delay in the performance of its obligations under this Agreement if such failure or delay is on account of causes beyond its control, including labor disputes, civil commotion, war, fires, floods, communicable disease, inclement weather, governmental regulations or controls, casualty, government authority, strikes, or acts of God, in which event Licensor shall be excused from its obligations for the period of the delay and for a reasonable time thereafter.

ABOUT THE RIMS RISK MATURITY MODEL®

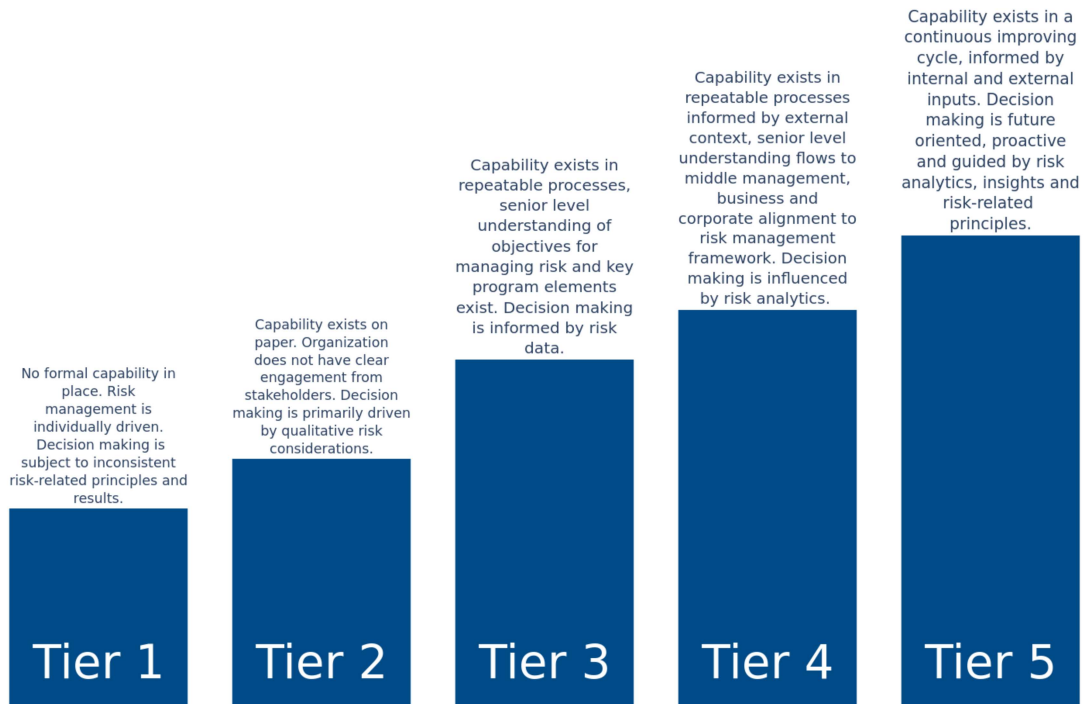
To develop the RIMS Risk Maturity Model® (RIMS RMM®), RIMS engaged with leading risk management professionals to redefine which elements (or pillars) and characteristics (or attributes) different organizations consider most important for achieving risk management maturity. The RIMS RMM® focuses on a continuum of team and organizational performance informed by these leaders’ experience and judgment in achieving continuous improvement. This model weighs its five pillars according to practitioners’ experiences with creating successful organizational outcomes. Each pillar is a necessary for successfully managing risk. The degree of criticality that each pillar contributes to organizational success differs, as reflected in the weights below. Each pillar is comprised of a number of attributes that also are assigned varying weights in the model.

	Pillar Title	Assigned Weight	Weighting Rationale Weights are derived from practitioner experience that most highly correlates with organizational success.
	Alignment with Strategy	25%	Alignment with strategy is the intersection of risk management insights and organizational purpose. Secondary only to culture, risk management that is aligned to strategy affects the whole enterprise and its entire value chain, anticipates dynamic forces and potentially alters the business model.
	Culture and Accountability	30%	Culture is how things get done; how decisions become actionable; how planning and performance occur. Culture takes a higher priority in risk mature organizations, as without this pillar the effectiveness of managing risk can be limited. With a more pervasive risk culture and respective accountability, organizational performance can be energized.
	Risk Management Capabilities	20%	Risk management capabilities reflect how well the entire organization manages risk. Organizational capabilities for risk assessment, analytic decision making and treatment options move from reliance on operational risk silos to a common methodology and strong competencies of participating stakeholders.
	Risk Governance	13%	Risk governance encompasses the institutional commitment, practices and arrangements that enable risk decision making. While risk governance provides a foundational structure within an organization’s normal governance structure, these arrangements have less affect on overall organizational success than other pillars.
	Analytics	12%	Analytics are the degree to which an organization uses technology and analytics to establish, collaborate, gain insight, and maintain connections with stakeholders. More sophisticated and timely risk analytics inform risk decisions and provide real-time actionable insights.

RIMS RISK MATURITY MODEL® Pillars



RIMS RISK MATURITY MODEL® Tiers



Overall Maturity Tier Results Compared to Target

The following pages describe your results for the pillar attributes as well as qualities of the next maturity tier. The target allows you to modify your organization's risk management practices for improving effectiveness.

Raw Average: 3.14

Weighted Average: 3.19

Your Risk Management Profile



Pillar 1 - Strategy Alignment



Target Tier: 4

Response Tier Weighted RMM Score: 3.33

- Process for integrating risk with decision making 3
- Extent of forward looking considerations 3
- Extent of risk evaluation for strategic initiatives or investment 3
- Consistency of risk appetite (risk and reward) and tolerance (acceptance of uncertainty or loss used in decision making) 3
- View of enterprise risk management capabilities within an organization 4
- Risk considerations of and to the business model 4

Maturity Tier Results Compared to Target

Target Tier: 4

Formal processes are used to consider risks after, during and before decisions are taken, i.e., assessing associated risk before decisions are taken such as before proceeding with an initiative, acquisition or new product launch. Execution is tracked and progress reported. Incorporates resilience sensitivity to extreme scenarios and disruptive forces (e.g. recession, epidemic, change of law, political instability). Risks for a strategic initiative or investment are evaluated continuously from early in the approval process with a risk treatment plan. Both appetite (risk/reward) and tolerance (acceptance of uncertainty/loss) are formally stated and considered as part of the planning process. Enterprise risk management capabilities are viewed as essential for success by most leaders in the organization, and risk reward tradeoffs are considered formally. Business model risks are analyzed and tested with the intent to verify or incrementally revise underlying assumptions or strategies.

Response Tier Weighted RMM Score: 3.33

Formal processes are used to consider risks after and during active decision-making i.e. in the context of maximizing success and minimizing failures in a project or initiative. Execution is tracked. Considers risks of future planned operations. Incorporates forecasts of usual drivers (e.g. competition, customers, cost, sales). Risks for a strategic initiative or investment are evaluated continuously from early in the approval process. Both appetite (risk/reward) and tolerance (acceptance of uncertainty/loss) are considered but not formalized. Enterprise risk management capabilities are viewed as additive for success by most leaders in the organization although risk/reward tradeoffs are not formally considered. Business model risks are considered to challenge underlying business model assumptions and possibly make tactical changes.

Pillar 2 - Culture and Accountability



Target Tier: 5

Response Tier Weighted RMM Score: 3.18

- Extent that results of risk assessments directly affect changes in initiatives, projects, or strategy 3
- Extent of direct contribution of employees and other stakeholders in collection of risk information 3
- Degree that risk considerations influence leadership 4
- Demonstration of risk culture oversight and accountability 3
- Connection between performance evaluation and managing risk 2
- Demonstration of leadership's understanding and accountability for managing top known risks 3
- Extent to which leaders actively participate in enterprise or organization-wide risk assessments 4

Maturity Tier Results Compared to Target

Target Tier: 5

Actions taken by owners of initiatives, projects and strategy to manage risk are considered as part of performance evaluation. Engagement for collecting risk information extends to include ecosystem of customers, suppliers, industry peers and others. Risk considerations occur before, during and after strategic and operational decisions are taken. Risk culture is agile, enabling an organization's proactive accountability and capability to adapt to dynamic ecosystem. Managing risk is considered a core competency and is included in individual and organizational performance evaluations for most levels of management. Most leaders hold themselves and their employees accountable for managing the top risks as well as understand the impact of the aggregate level of risk, where it is concentrated, and incorporate risk into decision making. Most leaders actively participate in enterprise risk assessments by volunteering information, offering differing perspectives, providing regular feedback and requiring risk assessments for major initiatives and strategy planning.

Response Tier Weighted RMM Score: 3.18

Assessment results are resourced and acted on by owners of initiatives, projects or strategy and reported to leadership. Contributions for risk information collection extend to middle management, and certain corporate functions (e.g., legal, finance, audit, strategy, planning). Risk considerations primarily occur in decisions related to operations (e.g., physical changes, employees, contracts, vendors). Leadership and/or governing body formally recognize ownership of the risk culture and individual accountability. Formal recognition program designed to reward individuals for identifying or managing risk to, of and from performance. Most leaders hold themselves and their employees accountable for managing the top known enterprise risks. Most leaders actively participate in enterprise risk assessments by volunteering information and offering differing perspectives.

Pillar 3 - Risk Management Capabilities



Target Tier: 4

Response Tier Weighted RMM Score: 3.00

- Considerations in evaluating risk treatments 3
- Level of analytical capabilities of organization and individuals in assessing risk 1
- Level of technical competencies of the organization's risk management leaders 3
- Assessment of emerging risks 4
- Span of developing and sharing risk information 3
- Extent of and criteria used in conducting enterprise risk assessments 4
- How well is the organization's risk profile understood? 3

Maturity Tier Results Compared to Target

Target Tier: 4

Alternate risk treatments are considered and evaluated based on underlying factors, root causes and likelihood of success. Organization demonstrates a strong ability to apply varying risk assessment techniques fit for purpose; able to provide training to risk assessors in multiple risk assessment techniques and estimation. Risk management leader is proficient in risk governance, designing data collection and reporting systems, interpreting risk interdependencies and consequences, and applying risk management techniques for strategy planning and implementation. Emerging risks are considered and assessed in a forward looking manner. Risk information is collected and shared through iterative consultation or discussions with leadership, board and internal stakeholders for decision making, and through formal methods, generally included in strategy performance reporting as well as operational reports. Assessments are based on common qualitative criteria, quantitative metrics and repeatable processes, regularly scheduled and informed by external and internal context and internal stakeholder engagement. Risk profile is well understood throughout the organization and is used as basis for organizational action.

Response Tier Weighted RMM Score: 3.00

Alternate risk treatments are considered and evaluated based on cost to control level of acceptable risk. Organization demonstrates strong ability to apply varying techniques for different purposes (e.g., perform probabilistic analysis and non-probabilistic sampling to create risk models); individuals are trained and proficient in multiple modeling techniques. Risk management leader is proficient in research, analytics, statistics, assessment methods and techniques, risk management information systems and financial analysis, data interpretation, behavior modification and risk modification techniques. Emerging risks are considered in a forward looking manner but they are not assessed. Risk information is collected and shared through iterative consultation or discussions with leadership and board for key projects and initiatives, and through formal methods, generally included in operational reports. Assessments are based on common qualitative criteria and repeatable processes, primarily driven by events; scheduled to meet regulatory requirements. Risk profile is centralized and understood by top management.

Pillar 4 - Risk Governance



Target Tier: 4

Response Tier Weighted RMM Score: 3.70

- Extent that organizational oversight responsibilities for risk management are established at the board or governing body level 5
- Extent that senior level leadership is committed, incented and rewarded for fostering value from risk management 3
- Degree that risk data process informs long term spending plans/decisions by leadership 3
- Development of a risk management function or framework 4
- Development of risk management policies or statements 4
- Extent that established operational or specialized (e.g. legal, insurance, safety) risk functions align with enterprise risk management function or framework 3
- Use of risk appetite considerations (e.g., risk return tradeoffs) 4

Maturity Tier Results Compared to Target

Target Tier: 4

Organizational risk management oversight responsibilities at board or governing body are formally and explicitly stated in internal and external-facing documents. Individuals are assigned formal and measurable risk management goals, use of tools, quantitative assessment and risk governance responsibilities. Formalized risk data process includes consultation with decision makers before options are determined and documented. A designated executive is responsible for developing and evolving the enterprise risk management function (e.g. CRO). Risk management statements or policies are in writing and are regularly reviewed. Risk appetite (risk return tradeoff) is applied using qualitative or quantitative factors consistently across the organization with thresholds generally set for multiple types of impact. Operational and specialized risk functions map to enterprise priorities. Risk appetite (risk return tradeoff) is applied using qualitative or quantitative factors consistently across the organization with thresholds generally set for multiple types of impact.

Response Tier Weighted RMM Score: 3.70

Organizational risk management oversight responsibilities at board or governing body are formally and explicitly stated in internal governance documents (charter, operating procedures, policies). Individuals are assigned specific performance goals and behaviors to promote enterprise risk management discipline. Formalized process and consistent use of risk data to communicate costs associated with planning. Leadership is engaged in recurring risk discussions (e.g. recurring agenda item) using common risk management approach or framework. Risk management statements or policies are in writing Operational or specialized risk functions exist and are loosely coordinated. Risk appetite (risk return tradeoff) is applied using qualitative factors consistently across the organization (e.g., thresholds generally set for potential financial losses).

Pillar 5 - Risk Analytics



Target Tier: 4

Response Tier Weighted RMM Score: 2.70

- Consistency of qualitative and quantitative analyses 3
- Extent that data and analytics are utilized to inform decisions about risk 3
- Extent that insights extracted from external sources and expertise are used to complement internal assessment data 4
- Extent that the influence of bias is considered in risk assessments 1
- Extent of varying methodologies and/or techniques used to identify and assess risks 2
- Thoroughness of assessing sources or causes of risk 3
- Availability of risk data to decision makers 2
- Depth and integration of risk reporting and communication within organization 3

Maturity Tier Results Compared to Target

Target Tier: 4

Organization analyzes most risks at the organizational level consistently using both qualitative and quantitative techniques. Data and analytics used within a formalized process with consistent application of analytical techniques applied in risk based treatment scenarios for informing enterprise risk decisions. Insights from external sources not involved with the organization (e.g., academia, World Economic Forum) are considered along with those directly and indirectly involved with the organization to complement internal risk assessment data. Impact of potential biases is managed through a formal process to assess possible impacts of bias on assessments. Use multiple qualitative methodologies/techniques and some quantitative methods, (e.g., simulations, stress testing) to identify, assess and validate risk. Organization applies root cause analysis techniques with specific risk indicators aligned and tracked. Standardized aggregated data exists that informs decision making within and outside the organization's business cycle. Reporting includes prioritization and evaluation of risk related controls, actions and timelines supported by KRI's and KPI's.

Response Tier Weighted RMM Score: 2.70

Organization applies analysis using largely qualitative techniques in some situations but not consistently. Data and analytics are used in specific situations with limited application in informing enterprise risk decisions. Insights are informed from current events (e.g. publications and news sources) to complement internal risk assessment data. Impact of potential bias in assessments is recognized but not managed. Primarily use surveys based on qualitative impact and frequency as assessment criteria. Organization relies on executive consensus without underlying root cause analysis. Risk data is segregated by business unit or function and not standardized across the organization. Reporting is aligned with external disclosures (e.g. risk factors and other external statements).

Risk Management Resources

Reading Recommended by Risk Management Professionals

Enable Strategy Alignment

- "A Board Perspective on Enterprise Risk Management," McK.insey Working Papers on Risk, Number 18, McK.insey & Company, 2010.
- Bridges, W. and Bridges, S., Managing Transitions, Making the Most of Change, Da Capo Lifelong Books, 5th edition, 2017.
- Kotter, J., Leading Change, Harvard Business Review Press, 2012.
- RIMS Executive Report, Exploring the Risk Committee Advantage, RIMS, 2015.
- RIMS Executive Report, Transitioning to Enterprise Risk Management, RIMS, 2014.
- RIMS Professional Report, Pivoting From ERM to SRM, RIMS, 2020.
- Spetzler, C., Winter, H., Meyer, J. Decision Quality: Value Creation from Better Business Decisions, John Wiley & Sons, Inc., 2016.
- Walker, P. L., Shenkir, W. G., and Barton, T. Establishing a Risk Challenge Culture. Strategic Finance, 2015.

Strengthen Risk Management Capabilities

- Fiorille , F., Graham, L., Kaufman, C., Identifying and Evaluating Emerging Risks, RIMS Executive Report, 2017.
- Fraser, J. and Simkins, B.J. Enterprise Risk Management, 2nd ed., John Wiley & Sons, Inc., 2021.
- Hopkin, Paul. Fundamentals of Risk Management; Understanding, Evaluating and Implementing Effective Risk Management, 5th edition, IRM, 2018.
- International Organisation for Standardization. Risk Management-Principles and Guidelines (ISO Standard No. 31000:2018) Handbook, iso.org, 2022.
- Lam, James. Enterprise Risk Management, 2nd ed., John Wiley & Sons, Inc., 2014.
- Lam, James Implementing Enterprise Risk Management: From Methods to Applications, John Wiley & Sons, Inc., 2017.
- RIMS Core Competency Model, RIMS, 2017.
- RIMS Professional Growth Model, RIMS, 2020.
- Sobel, P. and Reding, K. Enterprise Risk Management Achieving and Sustaining Success, The Internal Audit Foundation, 2012.

Integrate Risk Governance

- "A Board Perspective on Enterprise Risk Management," McKinsey Working Papers on Risk, Number 18, McKinsey & Company, 2010.
- "A Board Perspective on Enterprise Risk Management," McK.insey Working Papers on Risk, Number 18, McK.insey & Company, 2010.
- Bridges, W. and Bridges, S., Managing Transitions, Making the Most of Change, Da Capo Lifelong Books, 5th edition, 2017.
- Appelt, Dr. L., and Fox, C., Is Three a Crowd in GRC?, Risk Management Magazine, August 2019.
- Crickette, G. et. al, Exploring Risk Appetite and Risk Tolerance, RIMS Executive Report, 2012.
- Fiorelli, F. et. al, Steps to Successful Risk Taking: Developing Effective Risk Appetite and Tolerance Statements, RIMS ERM Committee Report, 2016.
- International Organisation for Standardization. Governance of Organisations (ISO Standard No. 37000:2022), iso.org, 2022.
- IRGC, International Risk Governance Council, An Introduction to the IRGC Risk Governance Framework. Policy Brief. Geneva: IRGC., 2007.
- Renn, O., Klinke, A. & van Asselt, M. Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis, Spring Link, 2011.
- Walker, P. L. Enterprise Risk and the Board of Directors. Business Horizons, 2014.

Incorporate Risk Analytics

- “A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis”, CIA, 2009 (access through Penn State University <https://www.e-education.psu.edu/sgam/node/155>).
- Bent, A. and Fox, C., Root Cause Analysis: More Than Just Cleaning Up the Mess, RIMS Executive Report, 2013.
- Chapman, R. Simple Tools and Techniques for Enterprise Risk Management, 2nd edition, John Wiley & Sons, Ltd, 2011.
- Fox, C. and Seigel, M. ANSI/ASIS/RIMS RA 1. Risk Assessment, ASIS & RIMS, 2015.
- HM Treasury, Risk Management Assessment Framework: A Tool for departments, 1st edition, 2009.
- Kahneman, D., Thinking Fast and Slow, Farrar, Straus and Giroux, 2011.
- Kahneman, D., Noise: A Flaw in Human Judgment, Little, Brown Spark, 2021.
- Merrifield, M., Innovation+ Strategic Risk Management: A Positive Pairing for a Better Future, RIMS Executive Report, 2020.

Influence Culture and Accountability

- Barton, T., Shenkir, W. G., and Walker, P. L. Making enterprise risk management pay off. Financial Executives Research Foundation, 2001.
- Berman, M., The Upside of Risk: Turning Complex Burdens into Strategic Advantages for Financial Institutions, Ncontracts, 2021.
- Chesley, D.L., et. al, COSO Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations, 2017.
- Gamble, John. Thompson Jr., Arthur; Peteraf, Margaret. Essentials of Strategic Management: The Quest for Competitive Advantage, 6th edition, 2019.
- International Organisation for Standardization. Risk Management-Principles and Guidelines (ISO Standard No. 31000:2018), iso.org, 2018.
- Pearce, John A. and Robinson, Richard B. Strategic Management Planning for Domestic & Global Competition, McGraw-Hill Education, 14th edition, 2014.
- Porter, Michael. Competitive Advantage, Free Press, 1985.
- Schwartz, P., The Art of the Long View: Planning for the Future in an Uncertain World, Bantam Doubleday Dell, 1991.
- Shenkir, W. G., and Walker, P. L., Enterprise risk management and the strategy-risk focused organization. Journal of Cost Management, 2006.
- Strategic Risk Management Development Council. RIMS Strategic Risk Management Implementation Guide, RIMS, 2012.

[Go to survey](#)



About RIMS

RIMS, *the risk management society*®, is a global professional association committed to advancing the practice of risk management throughout the world. We bring networking, professional development, certification, and education opportunities to our