International Labour Organization | ACT/EMP

Enterprise Risk Management

A Guide for EBMOs to promote efficiency and business resilience

Enterprise Risk Management

A Guide for Employer and Business Membership Organizations to promote efficiency and business resilience

January 2023

Bureau for Employers' Activities (ACT/EMP)

International Labour Office

First published 2023

Enterprise Risk Management. *A guide for Employer and Business Membership Organizations (EBMOs) to promote efficiency and business resilience*

English edition

International Labour Office – Geneva: ILO, 2023.

ISBN 978-92-2-038056-7 (web PDF)

Produced by the Publications Production Unit (PRODOC) of the ILO.
Graphic and typographic design, printing, electronic publishing and distribution.

The ILO endeavours to use paper sourced from forests managed
in an environmentally sustainable and socially responsible manner.
Code: CMD- REP

Preface

Volatility, uncertainty, complexity, and ambiguity characterize the business world today. The Global Risks Report 2022* shows the rise of multiple global risks, including economic, environmental, geopolitical, societal, and technological, with societal and environmental risks being perceived as the main short-term threats, followed by technological risks such as digital inequality and cybersecurity failure in the short to mid-terms. Moreover, the COVID-19 pandemic uncovered the vulnerability of enterprises to rare and unexpected events with significant consequences due to a lack of business continuity plans and insufficient financial buffers to cope with a drop in revenue caused by the sudden stop in economic activity to contain the propagation of the virus. This was particularly true for MSMEs in developing and emerging market economies.

In a business environment more prone to climate-related shocks and multiple global risks, enterprise risk management (ERM) will be more relevant than ever across enterprises, sectors, and countries to foster business resilience and preparedness for future crises. ERM is likely to become an indispensable pillar of best management practices for business continuity and long-term business viability, with significant implications on job creation and job retention.

In this context, Employer and Business Membership Organisations (EBMOs) can play a pivotal role in raising awareness among members about the importance of ERM and support them to develop ERM programmes using an integrated approach to navigate a multi-risks business environment.
This study prepared by the ILO Bureau for Employers' Activities is aimed at:

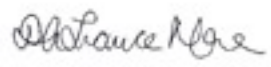
I. Reviewing what ERM is and why it matters.

II. Analysing the main features of ERM, the main implementation challenges, and best practices.

III. Providing guidance about what EBMOs can do to support their members in developing adequate ERM programmes according to best practices.

This report is mainly aimed at EBMOs as a thought piece for future action. However, it will also be of interest and relevance for all those interested in business resilience, business continuity, and an introduction to enterprise risk management. We remain at the disposable of our constituents to deepen this analysis and provide guidance in the pursuit of sustainable enterprises to create more and better jobs and raise standards of living.

Deborah France-Massin



Director
Bureau for Employers' Activities (ACT/EMP)
International Labour Office

* WEF (2022). Global risks report 2022. World Economic Forum.

Contents

Figures

Acknowledgements

This report, prepared by the ILO Bureau for Employers' Activities (ACT/EMP), benefited from the participation of several specialists who have collaborated in different phases of its development. First, we would like to thank Geoffrey Alles, Senior Consultant, for his meticulous work in reviewing the literature and drafting the report, which he co-authored.

Our thanks also go to José Luis Viveros Añorve, ILO-ACT/EMP Specialist, who managed the research process from design to implementation, provided technical contributions, and co-authored the report. We would also like to thank Roberto Villamil, Paolo Salvai, and Wade Bromley, ILO-ACT/EMP Senior Specialists, for reviewing the report and providing valuable comments to improve it.

▶ Introduction

Enhancing business productivity and resilience is a worthy goal. A healthy business environment benefits society, providing an ecosystem in which enterprises can thrive. Enterprises, when healthy and successful, provide decent and equitable employment, are an engine of economic growth, and pave the way for improved living standards. Employees and the consumers of their products and services alike benefit from sustainable enterprises, as does the entire stakeholder base. Forward looking enterprises are increasingly building sustainability into their business models. Yet the world we live in appears increasingly complex, fraught with unexpected dangers which can threaten enterprises' business models, brands and indeed their very existence.

We live in a world in which risk is ever-present. It has always been so. The concept of probability dates back thousands of years, bourn out of ancient games of chance. The game of backgammon is one of them and it is thought to date back some 5,000 years, originating in what is now southern Iraq. The foundation for modern probability theory was laid down by the French mathematicians Pascal and Fermat in the mid-seventeenth century in a series of letters they wrote together concerning games of chance (American Physical Society, 2009). Risk is essentially the level of possibility that an action or activity will lead to a loss or to an undesired outcome. The risk may even pay off and not lead to a loss, it may lead to a gain. Indeed, a certain level of risk is fundamental to the value proposition of most enterprises. A probability, on the other hand, is a measure or estimation of how likely is it that an event will come to pass, or that a statement is true. In relation to risk, probability is used to figure out the chance that a risk event will occur, an estimation as to its frequency. Thus, establishing the concept of probability was fundamental in the ability to formulate the notion of risk. Risk is ubiquitous. It is with us our entire lives, it can never be fully eliminated or avoided, and so we must learn to live with it.

The World Economic Forum publishes an annual Global Risks Report, breaking down risks into 5 broad categories: economic, environmental, geopolitical, societal, and technological. The risk profile of 2022 demonstrates a heavy concern for climate-based and environmental risk, followed closely by technological risk, such as digital inequality and cybersecurity failure (WEF, 2022). Contrast this with the profile of a decade ago, which highlights income disparity and fiscal imbalances as the top risks, and it becomes clear that risk is not static (WEF, 2021). Not only is it ever-present, it is also ever-changing. In an environment increasingly prone to climate shocks, black swan events and increasing global risks, how then is an enterprise to cope, to remain productive and resilient and not succumb to existential threats?

Countries, armies, and enterprises have always had risk managers, though they were not always labelled as such. The term "risk manager" arose out of the insurance industry in the 1950s (Rhodes, n.d.). For decades thereafter, companies would look primarily to insurance as a means to offload, or transfer, risk. Given the pervasive nature of the problem however, it became clear that risk transfer could only go so far before becoming prohibitively expensive. In the latter part of the twentieth century companies would normally assign ownership of risk to the managers of individual business units: the Chief Financial Officer (CFO) was responsible for financial and treasury risk, the Chief Operating Officer (COO) for production and distribution risk, and so on (Beasley, 2020). But what of risk occurring between business units, or risks in which the impact in one business unit appears relatively benign, but when aggregated across all business units becomes amplified, perhaps existential? These are but two of the many limitations of this silo-based approach.

A new methodology was required, and it evolved in the form of Enterprise Risk Management (ERM). In its most basic definition, ERM is risk management, but at the enterprise level. It starts with the very definition of the enterprise's strategic reason for being, and it seeks to identify, both qualitatively and quantitatively where possible, the top risks to the successful execution of the enterprise's strategy, whether they be internal or extrinsic. ERM seeks to strengthen an organization's processes with regards

to the identification, assessment, management and monitoring those risks most likely to impact the entity's strategic success. The evolving nature of the risk landscape and the ever-increasing complexity of the global business environment means that ERM cannot be viewed simply as a project, rather it must be seen as an ongoing process, flexible and ever vigilant for new and emerging risks which might impact the core objectives of the enterprise. The approach is top down, but it requires input from lower levels, and the considering of risk in all aspects of decision-making must be embedded within the very culture of the organization.

At first blush, the concept of a holistic approach towards risk may appear daunting, but it need not be. There are two primary frameworks upon which a company can draw as a roadmap for the development and implementation of an ERM programme. The first is the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management – Integrating with Strategy and Performance, originally issued in 2004 but updated in 2017 to strengthen the emphasis on the integration of ERM with strategy and performance. The COSO framework consists of five interrelated components: governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting (Claypole, 2021).

A second widely embraced framework is ISO's 31000:2018 Risk Management Guidelines, originally issued in 2009, and updated in 2018. ISO 31000:2018 focuses on six components: communication and consultation, scope and context, risk assessment, risk treatment, monitoring, and review, and recording and reporting (NC State ERM Initiative, 2020). Both frameworks share many of the same attributes, and while they are comprehensive in nature, they can be tailored to the needs of the individual organization and simplified to the point of becoming realistic, even for small and medium enterprises (SMEs). Chapter 1 of this report will identify the key steps and processes within each framework and identify areas of key competencies required to implement a successful ERM programme.

This report will also address the significant role that technology has to play in the development and implementation of an ERM strategy, by providing real-time information, making monitoring easier, helping to identify surface trends and making sure the escalation of a risk is flagged to the right people in the organization (Ten Six Consulting, 2018). From data collection and trend analysis to proactive risk dashboards and automated processes that can detect an escalating risk and introduce mitigation measures, technology is vital. Robotic Process Automation (RPA) can be used to improve data collection: more and better data can help an enterprise to identify and prepare for risk events. It can also improve risk analysis techniques such as regression and event tree analysis. Artificial Intelligence (AI) also has an important role to play in predictive analytics, with the potential to foster a high degree of predictive risk intelligence within an organization (Deloitte, n.d.).

Having laid the foundation for best practices in ERM in Chapter 1, Chapter 2 will offer pragmatic and real-world suggestions as to how EBMOs can advance the ERM process amongst their constituents, including amongst SMEs. Finally, existing tools, programmes and services currently offered by Employers and Business Member Organizations (EBMOs) will be examined with a view to identifying areas in which they can support their members with the development and implementation of their own individual ERM programmes. EBMOs can be a powerful advocate for positive change amongst its membership base. Many companies may not be aware of existential threats to their business; this was true with respect to climate change at least until recently. Many organizations, especially smaller ones, might not even be aware of the concept of ERM. EBMOs at the outset can raise awareness of the importance of having an ERM programme in place. Emphasis will be placed on assistance and support for SMEs, recognizing their importance as the majority segment of the world's economic activity. It is hoped that the concepts and ideas presented herein will translate to tangible improvements in business productivity and resilience in the real world.

References

American Physical Society, 2009. July 1654: *Pascal's Letters to Fermat on the*. [online] Aps.org. Available at: <https://www.aps.org/publications/apsnews/200907/physicshistory.cfm> [Accessed 2 May 2022].

Beasley, M., 2020. *What is Enterprise Risk Management (ERM)? | ERM - Enterprise Risk Management Initiative* | NC State Poole College of Management. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/library/article/what-is-enterprise-risk-management> [Accessed 2 May 2022].

Claypole, A., 2021. *The COSO ERM framework explained | Ideagen*. [online] Ideagen.com. Available at: <https://www.ideagen.com/thought-leadership/blog/the-coso-erm-framework-explained> [Accessed 2 May 2022].

Deloitte, n.d. *Seeing the Storm Ahead: Predictive Risk Intelligence*. [online] www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-seeing-the-storm-ahead.pdf> [Accessed 2 May 2022].

NC State ERM Initiative, 2020. *ISO's Risk Management Framework | ERM - Enterprise Risk Management Initiative | NC State Poole College of Management*. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/library/article/isos-risk-management-framework> [Accessed 24 April 2022].

Rhodes, A., n.d. *A Brief Summary of the Long History of Risk Management.* [online] Ventivtech.com. Available at: <https://www.ventivtech.com/blog/a-brief-summary-of-the-long-history-of-risk-management> [Accessed 2 May 2022].

Ten Six Consulting, 2018. *What Risk Management Technology Should You Use?.* [online] Ten Six Consulting. Available at: <https://tensix.com/what-risk-management-technology-should-you-use/> [Accessed 2 May 2022].

WEF, 2021. *The Global Risks Report 2021*. [online] www3.weforum.org. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf> [Accessed 2 May 2022].

WEF, 2022. *The Global Risks Report 2022*. [online] www3.weforum.org. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf> [Accessed 2 May 2022].

Enterprise Risk Management to enhance business productivity and resilience

Enterprise Risk Management to enhance business productivity and resilience

1.1. What is Enterprise Risk Management?

Enterprise Risk Management (ERM) is, in its simplest definition, risk management practiced at the enterprise level. It puts the core strategic mission of the enterprise at the centre of the discussion, driving all possible responses to potential risks in a holistic approach. This has not always been the case. The ever-increasing complexity of the world is engendering new and sometimes previously unimagined risks, ones that don't always fall within what was considered traditional risk management practice. The need for a different approach had become increasingly clear over the last two decades or so, and ERM emerged to the fore as a response to these new challenges. ERM is still evolving, a fitting testament to the fact the ERM is itself an ongoing process and not a one-time project. This section will describe the history of risk management as a backdrop to better understand what is now considered cutting-edge ERM.

1.1.1. Historical risk management practices and their limitations

Today's risk managers are concerned with the impact of future events and their likelihood of coming to pass. However, it can also be instructive to look at the past to better shape future decisions. The concept of risk, and with it the idea of probabilities dates back thousands of years. Tribal priests of different ancient civilizations would roll bones to predict the future, and their peoples would invent and play games of chance with bones and eventually dice. Backgammon is thought to date back some 5,000 years, originating in what is today southern Iraq.

There is historical evidence that gambling gave rise to the probability theory of today, and indeed to the concept of risk itself. In mid-17th century France, an exchange of letters occurred between two prominent mathematicians, Blaise Pascal, and Pierre de Fermat, on "the problem of points." The question was posited by Antoine Gombaud in 1654, an amateur mathematician who was fond of gambling. Pascal and Fermat realized that the question required a new form of mathematical analysis, and they succeeded in laying the foundation for modern probability theory and forever changing the views of scientists and mathematicians on probability and risk (American Physics Society, 2009).

In his book Against the Gods: The Remarkable Story of Risk, Peter Bernstein suggests that the dividing line between what may be considered ancient times and modern times is that of embracing the concept of risk, that everything was not pre-ordained by the gods or the whims of nature. It was this understanding of the inevitable variability of future outcomes and events that unshackled probability and risk from the alternate view of the mystics and the priests. Bernstein later recounts the story of Nobel laureate Kenneth Arrow who served in the U.S. Air Force during the Second World War and was tasked with forecasting the weather months in advance. This was at the time nothing more than guesswork. When Arrow argued that the forecasts were useless and should be discontinued, the reply came back: "*the Commanding General is well aware that the forecasts are no good. However he needs them for planning purposes*" (Bernstein, 1998).

For almost as long as there have been countries and enterprises there have been people within those entities dedicated to managing risks, using whatever tools they might have had at the time. The first actuaries worked in what was to become

a modern life insurance company in England as far back as the 1700s. Henri Fayol, known for writing one of the first works on the theory of business administration in 1916 has since been recognized by some academics as an early thought leader on risk management. The term "Risk Manager" came to the fore in the insurance industry in the 1950s, where risk managers had the tasks of identifying risks and estimating probabilities, to provide a basis for policy pricing. The discipline spread to other industries, where risk managers would usually turn to insurance to offset risk. Risk however is systemic, pervasive, ever-present. It is impossible to offset every risk with insurance. It was clear that risk could not be avoided, it had to be lived with. A new approach was needed.

From the 1970s until relatively recently, enterprises set about to tackle risk management with a silo-based, or stove pipe approach. This structure towards managing risks meant that the executives in charge of each of the various business units within an organization would be responsible for risks within their individual business units. Thus, the Chief Marketing Officer was responsible for risks and the management thereof with respect to sales and customer service. The COO owned risks associated with production and distribution, as did the CFO with aspects of finance and treasury, and so on across the organization (Figure 1).

▶Figure 1: Traditional silo-based approach to risk management

Source: Beasley, 2020.

There are however serious limitations with such a strategy. Risks do not adhere to the organizational chart of an enterprise, and they may fall between the silos and go unnoticed by business unit leaders until a catastrophic event is triggered. As an example, external changes to the regulatory, legal and compliance department may go unnoticed by the CFO until the effects show up on the bottom line. In a retail organization, demographic shifts in the population may go unnoticed by the marketing unit, resulting in the misallocation of real estate resources. Risks that fall between the silos can be seriously detrimental to the value proposition and strategic direction of the business.

In the silo-based approach there are risks that might be seen as relatively innocuous to individual leaders of a business unit that might set up to become a strategic threat to the enterprise when amplified by their cumulative impact on different areas of the organization. For example, a new distribution strategy might be considered in relocating a warehouse to a different jurisdiction, or even a different country. Has the legal and compliance department been given sufficient time to weigh in? What of different tax implications of varying jurisdictions to finance and treasury? If all of the individual business units are aligned, it becomes relatively easy to see that better decisions are the likely outcome.

A third limitation is that the owners of individual silo-based risk may make seemingly rational risk responses for their own business units, but the same such responses might have unintended consequences to other areas of the

business. What if an IT department that seeks to aggressively deter cyber security threats but in doing so alienates the online customer base through a less user-friendly interface? Such an action might represent a perfectly reasonable decision by the IT department in a vacuum, but the risk to the enterprise itself could prove to be substantial.

When the lens of risk management is directed only towards individual units, it is fair to ask what then of externally generated risks to the business? Is there anyone tasked with taking a wider external view? It has long been acknowledged in business management theory that a solid competitive analysis is foundational to the success of an enterprise. This sometimes takes the form of a SWOT analysis – strengths, weaknesses, opportunities, threats – and such an understanding of the ever-changing competitive landscape is often fundamental to the very survival of an enterprise. It may be as simple as a competitor's new product or technology on the horizon, but one with the potential for massive disruption of an individual company's current offering. Examples of risks that might not be captured by the silo approach include:

- Demographic shifts in the market
- Competitive risks via new products, services, and technologies
- Geopolitical developments that might restrict access to markets, including conflict and war
- Risks in a changing regulatory environment where a new jurisdiction might be being considered as part of the strategic plan
- Risk in attracting and maintaining skilled employees in a competitive labour market
- Exogenous risks to the supply chain
- Risks of the resurgence of the COVID-19 pandemic and of future pandemics

As mentioned, the taking on of risk is itself fundamental to the value proposition of an enterprise. The deployment of capital, irrespective of the amount, is inherently risky. Simply opening the doors of a business is fraught with risk. Risk therefore has to be recognized and managed. An organization must make sure that its approaches to risk management are in lockstep with the organization's strategic goals and mission, and not simply internalized to individual business units. Business leaders are increasingly describing what they view as a more complicated risk environment, suggesting that it is useful to comment upon the changing global risk landscape (Branson, Beasley and Hancock, 2019).

1.1.2. The changing global risk landscape

The World Economic Forum (WEF) publishes an annual Global Risks Report typically breaking down known risks into five broad categories: economic, environmental, geopolitical, societal, and technological. The overview of what the WEF considers to be known risks for 2022 is presented in Appendix 1. The global risk perceptions are meant to be all-encompassing, though one might argue that some risks can't be known or seem so far-fetched that they don't seem worthy of consideration. It is extremely difficult, perhaps impossible, to anticipate everything that might possibly occur.

Rather than simply describing the possible risks knowable in 2022 or in any other year, a more informative exercise is to look at how risk perception has evolved in the WEF annual global risks report over the last decade. Going back to 2012 for example, the risks with the greatest likelihood of occurring were seen to be income disparity and fiscal imbalances, only then followed by GHG emissions and cyber security. Fast forward to 2021 and the top four most likely risks were deemed to be extreme weather events, the failure to take adequate action on climate change, and human environmental damage, followed by infectious diseases. It is interesting to note that the risk of infectious disease ranked in the top four in 2021, yet it wasn't even on the radar as a likely scenario a decade ago (Figure 2). The Obama administration wrote a pandemic playbook and put the medical and scientific professionals in place; the Trump administration dismantled the

office and threw the playbook in the dustbin. Had the likelihood of a pandemic changed? Arguably it had not, suggesting that the perception of risk may itself be somewhat fickle, particularly when it involves people in positions of significant power. The same can be said of both governments and corporations.

▶Figure 2: Evolving risks landscape

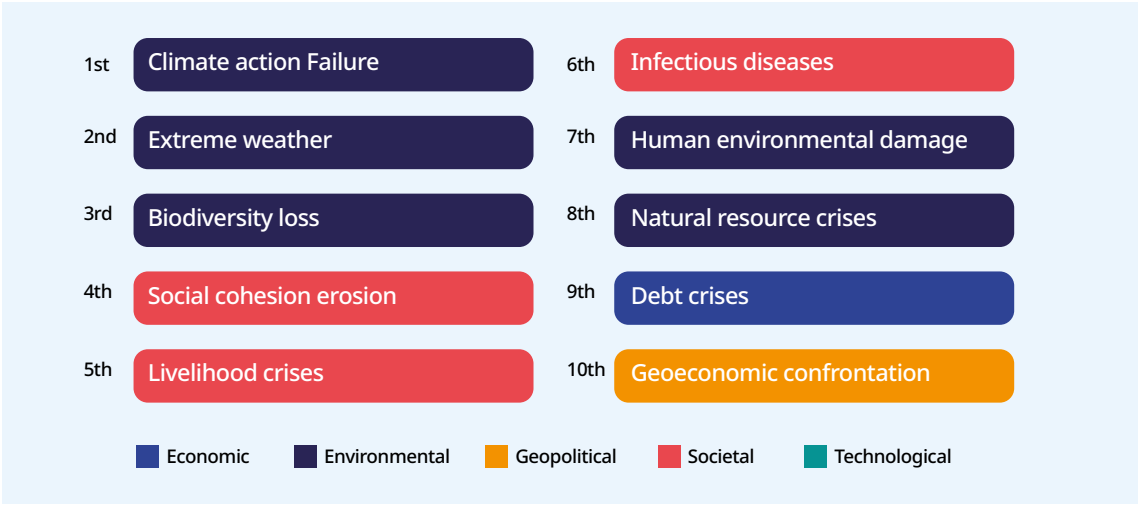
Top Global Risks Likelihood

	1st	2nd	3rd	4th	5th	6th	7th
2021	Extreme weather	Climate action failure	Human environmental damage	Infectious diseases	Biodiversity loss	Digital power concentration	Digital inequality
	1st	2nd	3rd	4th	5th		
2020	Extreme weather	Climate action failure	Natural disasters	Biodiversity loss	Human-made environmental disasters		
2019	Extreme weather	Climate action failure	Natural disasters	Data fraud or theft	Cyberattacks		
2018	Extreme weather	Natural disasters	Cyberattacks	Data fraud or theft	Climate action failure		
2017	Extreme weather	Involuntary migration	Natural disasters	Terrorist attacks	Data fraud or theft		
2016	Involuntary migration	Extreme weather	Climate action failure	Interstate conflict	Natural catastrophes		
2015	Interstate conflict	Extreme weather	Failure of national governance	State collapse or crisis	Unemployment		
2104	Income disparity	Extreme weather	Unemployment	Climate action failure	Cyberattacks		
2013	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Water crises	Population ageing		
2012	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Cyberattacks	Water crises		

Source: WEF, 2021.

In 2022, the perceived risk likelihood landscape shifted again, and while climate-related issues stayed at the fore, the perceived risk of infectious diseases dropped off considerably (Figure 3). But has the risk really changed that significantly? The fact that the risk of a pandemic was not taken seriously meant that most countries and companies did not have access to, nor the capacity to manufacture, simple PPE. It would not be far-fetched to suggest that, given the events unfolding in Ukraine at the time of writing, the risk of geopolitical strife and war is likely to rank highly in 2023's WEF report. What are we to make of this, and why are we seemingly raising our perceptions of the likelihood of a risk event only after the fact?

▶Figure 3: Perceptions of likelihood of risk events in 2022 over the next ten years



Source: WEF, 2022.

The problem is exacerbated by the fact that many business leaders of the largest corporations are seemingly entirely out of sync with the WEF. The ERM Initiative in the Poole College of Management at North Carolina State University also does an annual survey of boards of directors and C-suite executives on their perception of risks for the upcoming year. In 2022 that survey compared top executives' risks perceptions in both 2022 and for ten years from now, in 2031 (Figure 4). Upon closer inspection it appears that most of those executives surveyed tended to be rather inward-looking in their approach to risk.[1] There was clear focus on operational issues, the ability to hire and retain skilled employees and what can almost be read as a fear of their ability to cope with big data.

The WEF 2022 report highlights climate-related issues as five of the top ten risks deemed most likely; in the Poole survey, climate does not even register in the top ten, now or in a decade from now. It can be legitimately argued that the risks of climate change are existential, to governments, industries, enterprises, EBMOs, indeed to us all. It is disturbing that these C-level executives do not seem to be focused on the severity of the threat. In the short-term adaptation measures to climate change are prudent. Longer term mitigation efforts are themselves existential. The Poole study also recognized some ongoing pandemic-related risks in 2022, but not any in 2031. Will the risk of another pandemic significantly diminish over the coming decade? Probably not, given the ever-increasing encroachment of human habitats upon the natural environment. The same can be said of technological risks, including cyber security and the hacking and coopting of networks in both infrastructure and business. The WEF in 2022 highlights that our growing digital dependency only serves to intensify cyberthreats. It is important to note that the WEF results are looking ahead ten years. In the Poole study cyber risks are identified in 2022, but not so in 2031. If the risks lens is indeed so intrinsically focused, it is difficult not to conclude that many of these executives are too heavily entrenched in traditional risk management practices, and not in maximizing the value proposition of their enterprises by not preparing for exogenous and potentially existential threats.

1 The Poole survey included 1,423 board members and executives across a variety of industries, including 43% with operations in North America, 20% in Europe, 20% in Asia and Australia/New Zealand, and the remaining 17% from Latin America, India, Africa and the Middle East.

▶Figure 4: Poole study comparing top risks identified by business leaders in 2022 and 2021

Top risks for 2022	Top risks for 2031
1. Pandemic-related government policies and regulation impact business performance	1. Adoption of digital technologies requires new skills or significant efforts to upskill/reskill existing employees
2. Succession challenges, ability to attract and retain top talent	2. Succession challenges, ability to attract and retain top talent
3. Pandemic-related market conditions reduce customer demand	3. Succession challenges, ability to attract and retain top talent
4. Adoption of digital technologies requires new skills or significant efforts to upskill/reskill existing employees	4. Substitute products or services arise that affect our business model
5. Economic conditions, including inflationary pressures, constrain growth opportunities	5. Economic conditions, including inflationary pressures, constrain growth opportunities
6. Increasing labor costs impact profitability targets	7. Entrance of new competitors and other industry changes threaten market share
8. Resistance to change operations and the business model	7. Impact of regulatory change and scrutiny on operational resilience, products, and services
8. Inability to utilize data analytics and “big data” to achieve market intelligence and increase productivity and efficiency	8. Resistance to change operations and the business model
9. Cyber threats	9. Hybrid work environment and changes in nature of work challenge ability to compete
10. Shifts in expectations about social issues and diversity, equity and inclusion (DEi) outpace organization’s response	10. Inability to utilize data analytics and "big data• to achieve market intelligence and increase productivity and efficiency

Source: NC State ERM Initiative, 2022.

1.1.3. State-of-the-art ERM is impacting how businesses cope with a rapidly changing world

It is clear from the above that some business leaders have seemingly been heavily reliant on the traditional silo-based risk management approach, and that major exogenous shocks have not been adequately anticipated nor prepared for. The two most recent shocks, namely the pandemic and Russia’s war in the Ukraine can be considered as black swan-type events with deep underlying reverberations. The pandemic for its part has resulted in supply chain chaos, labour shortages and inflation. The conflict in Ukraine has resulted in sanctions, the closing of the operations of many western enterprises, food insecurity, and the weaponization of Russian energy sources, just to name a few. It is beyond the scope of this paper to analyse theses impacts, though they are likely to ripple through generations to come. Rather, it is important to demonstrate that in most cases these risks were never adequately identified nor prepared for in the first place. The fact that business leaders and other stakeholders have seemingly come to raise their perception of the likelihood of certain risk events only after the fact is clearly not helpful. This backward-looking approach is unlikely to build sufficient resilience for future unexpected and black swan-type events, nor serve to enhance the value of the enterprise.

The need for a different approach has become increasingly clear over the last two decades or so and ERM has emerged to the fore as a response to these new challenges. As

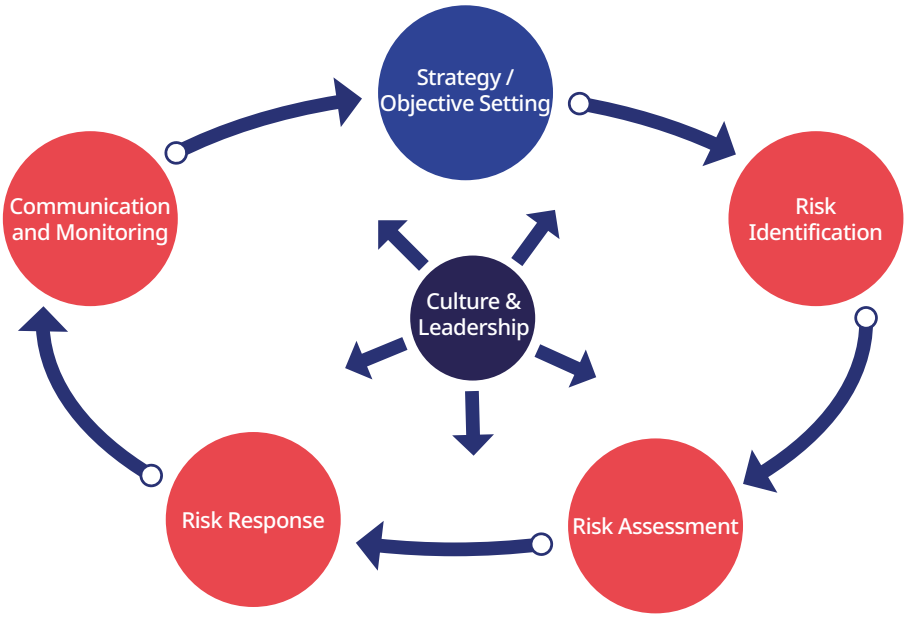
aforementioned, Enterprise Risk Management (ERM) is, simply put, risk management practiced at the enterprise level. It puts the core strategic mission of the enterprise at the centre of the discussion, driving all possible responses to potential risks in a holistic approach. Not all business leaders are trapped in the past of course, as ERM has been evolving in the understanding of its value and importance. The NC State ERM Initiative has partnered over the past ten years with the American Institute of Certified Public Accountants' (AICPA) Management Accounting - Business, Industry, and Government Team to survey business leaders regarding a number of characteristics related to their current enterprise-wide risk management efforts. Their 2019 Report on the State of Risk Oversight collected data from some 500 or so large organizations, and found that, while most executives perceive that uncertainties in the business environment are leading to more complex risks over time, they are particularly concerned about risks related to talent, innovation, the economy, and their reputation and brand.

This suggests once again that the risk lens is being focused too internally and is failing to account for external, possibly existential shocks. It is interesting to note that risk related to the impacts of climate change climate change were absent from those views. The report also found that the majority of these organizations indicated they had recently experienced an operational surprise due to a risk they did not adequately anticipate. The study also concluded that external stakeholders are increasingly demanding greater senior executive involvement in risk management and that more organizations are appointing an executive to oversee their risk management processes, with most organizations creating a management-level risk committee. It was found that roughly half of the organizations do engage in formal risk identification and risk assessment analysis, yet very few believe that their approach to risk management is actually providing any strategic value. Tellingly, the report also concluded that perceived roadblocks are impeding organizations from enhancing their risk management practices is the belief that the costs associated with an enterprise-wide risk management process are likely to exceed the benefits, and that there are too many competing priorities (Branson, Beasley and Hancock, 2019). These inconsistencies, between belief and action, illustrate that much remains to be done. EBMOs will have an extremely important role to play in this respect, as will be more fully explored in Chapter 2.

ERM thus seeks to identify, both qualitatively and quantitatively where possible, the top risks to the successful execution of the enterprise's strategy, whether they be internal or extrinsic. Section 1.1.2 demonstrated the evolving nature of the risk landscape. The ever-increasing complexity of the global business environment means that ERM cannot be viewed simply as a project, rather it must be seen as an ongoing process, flexible and ever-vigilant for new and emerging risks (and sometimes opportunities) which might impact the core objectives of the enterprise.

ERM seeks to strengthen an organization's processes with respect to the identification, assessment, management and monitoring those risks most likely to impact the entity's strategic success (Figure 5). This starts with the definition of an enterprise's core strategy, its mission statement, its very reason for being. The approach is top down, involving both the board and its C-level executives, but it requires input from lower levels, and the considering of risk in all aspects of decision-making. ERM must be embedded within the very culture of the organization in the furtherance of its core objectives.

▶**Figure 5: Elements of an ERM process**



Source: Beasley, 2020.

Once an organization has clearly identified and communicated its strategic objectives, the next step in the process is the identification the top risks that might threaten to derail the execution of a business' core strategy. The list does not have to be overly comprehensive. The priority should be to identify those risks that are most likely to have the most impact. This might normally involve 8 – 15 or so top risks, depending upon the complexity of the enterprise (Hancock, 2015). The question then becomes how to go about the process risk identification, and how to assess those risks, considering such factors as an organization's risk appetite, and the impact and likelihood of a risk event to occur. The risk response must then be addressed, usually by one of four means: avoidance, transfer, mitigation or acceptance (Moeller, 2007). Communication and monitoring are essential in providing feedback with respect to the core objectives, and the process becomes a continuous loop, with ERM leadership and risk culture at the centre of it all. Section 1.3 will explore the development of each of these elements within an ERM programme that can be tailored to the specific needs and complexities of the organization. Firstly however, a look at the evolution of ERM frameworks provides an insightful backdrop before designing a specific ERM programme.

1.2 ERM frameworks

First considerations for a need for an ERM approach to risk may be somewhat daunting to many executives new to the process. The adoption of a holistic approach to risk management is inarguably more complex than traditional methods. Fortunately, companies can relay on two key and widely-recognized frameworks to serve as a roadmap and help devise a strategy. The first structural depiction of an ERM framework was detailed in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management – Integrating with Strategy and Performance, originally issued in 2004. The 2004 version was later updated in 2017, to strengthen the emphasis on the integration of ERM with strategy and performance. The updated COSO framework consists of five interrelated components: governance and culture, strategy and objective-setting, performance, review and

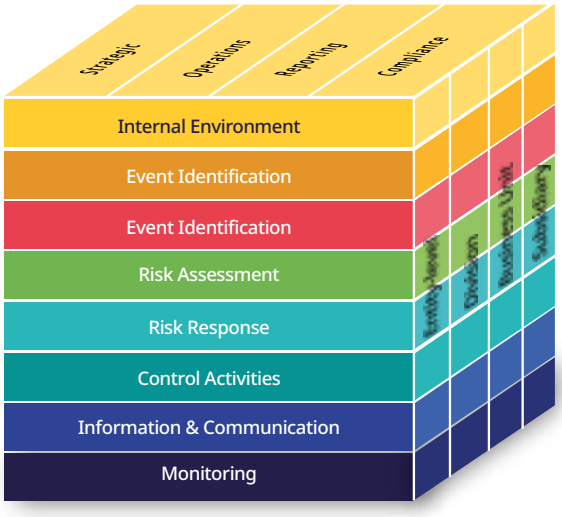
revision, and information, communication and reporting (Claypole, 2021).

A second widely embraced framework is ISO's 31000:2018 Risk Management Guidelines, originally issued in 2009, and updated in 2018. ISO 31000:2018 focuses on six components: communication and consultation, scope and context, risk assessment, risk treatment, monitoring and review, and recording and reporting (NC State ERM Initiative, 2020). Both frameworks share many of the same attributes, and while they are comprehensive in nature, they can be tailored to the needs of the individual organization and simplified to the point of becoming realistic, even for SMEs.

1.2.1. Guidance provided by the COSO ERM cube 2004

The COSO ERM cube provided the first framework against which risk management and internal control systems could be assessed and improved. The cube is reproduced here in Figure 6. Essentially the cube depicts the core strategic objectives of the enterprise on the top surface, and links them to eight categories on the front face, representing key components of an ERM strategy. The third dimension represents individual business units, suggesting the need for ERM to be fully embedded within an organization's culture and implemented across all activities within the enterprise.

▶Figure 6: COSO 2004 ERM Framework Cube



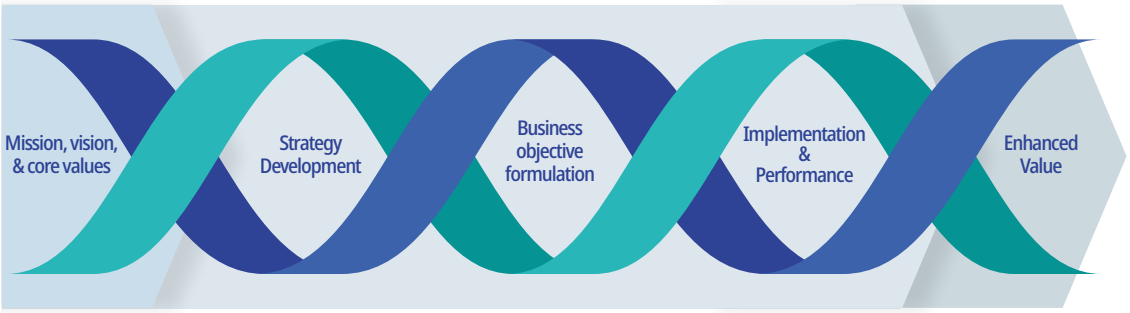
Source: IRM, n.d.

The internal environment sets the cultural tone of the organization and influences attitudes towards risk management, risk appetite and ethical values. The guidance considers the impact of the competitive environment, regulation and external stakeholders on risk appetite and culture. Objective setting seeks to define the core strategy of the enterprise, and to ensure that strategy is thoroughly disseminated across the organization. The organization must then seek to identify internal and extrinsic risks to the execution of its core mission. Risks then need to be assessed both in terms of their potential impact and their likelihood. Senior management must then develop a response to a risk event, based upon their risk appetite and tolerance. Control activities are designed to ensure that risk responses are effective. Information needs to be fed back to senior management and the entire process should be monitored, and if necessary, modified.

1.2.2. Guidance provided by the COSO framework 2017

The COSO ERM cube was the first illustration of the interdependencies involved in an enterprise-based approached to risk. It also formed the basis for COSO's revised 2017 framework (Figure 7), which placed added emphasis on the integration of strategy and performance, i.e. productivity. It is intended to ensure that strategy is not misaligned with core values and the strategic mission, and that if such misalignment occurs, there is sufficient internal information and feedback to allow for a reset. The 2017 guidance also places additional emphasis on risk appetite and tolerance. Finally in the event that the ERM process results in a need to alter core strategy, each new strategy will in turn have a different risk profile, reinforcing the need for continuous feedback in an ongoing process (Martens and Rittenburg, 2020).

▶**Figure 7: COSO 2017 ERM framework Double Helix**



Governance & culture	Strategy& Objective-Setting	Performance	Review & &Revision	Information, Communication & Reporting
1. Exercises Board Risk Oversight	6. Analyzes Business Context	10. Identifies Risk	15. Assesses Substantial Change	18. Leverages Information and Technology
2. Establishes Operating Structures	7. Defines Risk Appetite	11. Assesses Severity of risk	16. Reviews Risk and Performance	19. Communicates Risk Information
3. Defines Desired Culture	8. Evaluates Alternative Strategies	12. Prioritizes Risks	17. Pursues Improvement in Enterprise Risk Management	20. Reports on Risk, Culture. and Performance
4. Demonstrates Commitment to Core Values	9. Formulates Business Objectives	13. Implements Risk Responses		
5. Attracts, Develops, and Retains Capable Individuals		14. Develops Portfolio View		

Source: IRM, n.d.

The COSO 2017 ERM double helix consists of four top-level components, beginning with mission, vision and core values, which leads to strategy development, the setting of objectives, and finally implementation, all of which are designed to result in enhanced enterprise value. Residing below these primary elements are five guiding principles: Governance and Culture; Strategy and Objective-setting; Performance; Review and Revision; and Information, Communication and Reporting. Governance and culture seek to develop the overall tone of senior management towards ERM, and developing a consistent culture, promoting desired behaviours, and instilling ethical values. Strategy and objective-setting offers guidance on establishing the appetite

for risk, formulating strategic objectives, and establishing the means to properly identify, assess and respond to key risks. Performance looks to identify the potential severity of risks and develop appropriate responses towards those risks. Review and revision allow organizations to reflect upon the ERM processes and to examine how well their ERM programme is functioning. If the risk landscape has evolved, enterprises can determine where modifications and improvements can be made. Finally, information, communicating and reporting relies increasingly on technology to provide constructive information that can be fed back into the ERM process (Claypole, 2021).

The 2017 COSO guidance also seeks to enhance enterprise resilience. In identifying various risks, enterprises are also finding opportunities, and areas for change that might enhance productivity and strategic success. Identifying avenues for change also can suggests important shifts in strategy. Core strategy must always be under review as a part of the ERM feedback loop. Strategy needs to be periodically adjusted, based not only upon an evolving risks landscape, but also by being aware of ever-changing new opportunities that may further enhance enterprise value.

1.2.3. Guidelines provided by ISO 31000: 2018

A second widely embraced framework is ISO's 31000:2018 Risk Management Guidelines, originally issued in 2009, and later updated in 2018. It is also commonly referred to as Annex SL. ISO 31000:2018 focuses on six components: Communication and Consultation emphasizes the importance of creating awareness and the understanding of risk, not only within the organization, but across the entire stakeholder base. Scope, Context and Criteria highlight the need for ERM to be designed with the specific needs of the organization in mind. Risk Assessment includes risk identification, analysis and evaluation. Risk Treatment refers to the risk response (avoidance, transfer, mitigation, acceptance). Monitoring and Review identifies the importance of collecting the information necessary to improve the effectiveness of the ERM programme. Finally, Recording and Reporting disseminates that information to the proper individuals such that appropriate actions can be undertaken. The core components are underpinned by a series of principles designed to ensure that risk management is fully integrated across the enterprise, that it is structured to ensure consistency, and that it is customized to the organization. ERM must also include input from all key stakeholders and be flexible enough to adapt to an ever-changing risk landscape (NC State ERM Initiative, 2020). Although the reporting structures are inherently different each of the COSO frameworks and ISO 31000, they are in fact attempting to provide similar guidance. A detailed comparison of the COSO frameworks and ISO's Annex SL is presented in Appendix 2.

1.3. Best practices in ERM programme development

The development of and ERM programme is individual to the enterprise, and requires a custom approach, considering factors such as the mission statement of the enterprise, its size, its complexity, its resources both human and capital, and such other factors as might be intrinsic to the specific organization. This section will look at best practices in the development of a state-of-the-art ERM programme. As noted, an ERM strategy begins with the strategic objective. An ERM programme can then be divided into four additional components as seen in Figure 5: risk identification, risk assessment, risk response, and communication and monitoring. This section will take a closer look at each of these components.

1.3.1. Risk identification

ERM is a continuous feedback loop, ever evolving, but a business needs to start somewhere. This is normally with the process of risk identification. Most enterprises begin by developing an overall risk inventory that seeks to provide a comprehensive list of risks to the organization. Identifying potential risks is distinct from assessing those risks, although the lines can sometimes be blurred. Accurate risk definitions are critical to the overall success of an ERM

programme, particularly in environments where there is little supporting data. The risk identification process will usually involve input from the managers of individual business units, but it also requires senior management and the board to cast a broad net to capture the universe of risks facing the enterprise. To identify these risks, interviews can be conducted across the C-suite, and surveys can be designed for business unit managers, and depending upon the complexity of the organization, one or two levels below. Once input and data is collected it should be challenged by way of internal meetings and debate to arrive at as accurate a depiction of the holistic risk landscape as is possible. These risks can then be organized by risk category, such as strategic, financial, operational, etc., and by sub-categories for individual business units. Risk identification is a starting point, but a universal depiction of risks is not in and of itself practical for the development of an ERM programme. These risks need to be assessed and prioritized into a manageable number of risks, as referenced usually on the order of 8 to 15 or so top risks, which can then become the focus for a detailed and planned response.

1.3.2. Risk assessment

Risk assessment is itself a detailed process, and according to COSO it can be broken down into four key components: developing risk assessment criteria, assessing risks, assessing risk interactions, and ultimately prioritizing those risks (Figure 8). A homogenous set of assessment criteria is integral to the risk assessment process. It must be consistent across all business units and the enterprise as a whole if it is to useful in aggregating risks across the enterprise as a whole. In broad terms organizations typically assess risk based on two criteria: overall impact to the enterprise, and the likelihood of its occurrence. In a survey of risk assessment practices, Hancock (2015) found that advisory board members use a variety of different dimensions in assessing risk in addition to those above, including velocity (i.e. how quickly the risk event will occur), persistence (how long the negative consequences of the risk event are expected to last), and interdependency (how much influence does a risk have on the occurrence of other risks). In other words, impact and likelihood don't tell the whole story. A business also needs to consider both its vulnerability to a particular risk, and its speed of onset. Once an enterprise understands its potential vulnerability, it becomes possible to paint a clearer picture of the organization's needs. Gauging the velocity of a risk can then highlight the need for agility and rapid adaptation.

▶**Figure 8: Risk assessment process**

Source: Curtis and Carey, 2012.

Assessing risk usually means assigning values to each risk using a unique set of defined criteria tailored to the organization. The process usually encompasses both a qualitative and a qualitative component: an initial qualitative screening of risks precedes a more quantitative analysis of those risks deemed most important to the enterprise. In some industries, such as the financial industry it is sometimes possible to quantify risks in monetary terms. In most instance however, organizations develop scales to rate risks that might otherwise be unquantifiable. Scales allow for a uniform form of measurement that can be used across the organization, and if employed consistently, can be used to aggregate risk across the organization. Scales usually involve a ranking based upon several points, with most enterprises using a five-point scale as sufficiently representative without become too detailed or unwieldly. In its thought paper on risk assessment practices, Curtis and Carey (2012) of Deloitte suggest the inclusion of scales based upon each of impact, likelihood, vulnerability and speed of onset as sufficiently representative for

most organizations (Figure 9). However different scales can be customized to the needs of the individual enterprise as required.

▶Figure 9: Illustrative risk scales for impact, likelihood, vulnerability, and speed of onset

Illustrative Impact Scale

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines. litigation including class actions. incarceration of leadership • Significant injuries or fatalities to employees or third parties. such as customers or vendors • Multiple senior leaders leave
4	Major	• Financial loss of $X million up to $X million • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as customers or vendors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	• Financial loss of $X million up to $X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as customers or vendors • Widespread staff morale problems and high turnover
2	Minor	• Financial loss of $X million up to $X million • Local reputational damage • Reportable incident to regulator, no follow up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increase in turnover
1	Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties. such as customers or vendors

Illustrative Likelihood Scale

Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
5	Frequent	Up to once in 2 years or more	Almost certain	90% or greater chance of occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life of asset or project

Illustrative Vulnerability Scale		
Rating	**Descriptor**	**Definition**
5	Very High	• No scenario planning performed • Lack of enterprise level/process level capabilities to address risks • Responses not implemented • No contingency or crisis management plans in place
4	High	• Scenario planning for key strategic risks performed • Low enterprise level/process level capabilities to address risks • Responses partially implemented or not achieving control objectives • Some contingency or crisis management plans in place
3	Medium	• Stress testing and sensitivity analysis of scenarios performed • Medium enterprise level/process level capabilities to address risks • Responses implemented and achieving objectives most of the time • Most contingency and crisis management plans in place, limited rehearsals
2	Low	• Strategic options defined • Medium to high enterprise level/process level capabilities to address risks • Responses implemented and achieving objectives except under extreme conditions • Contingency and crisis management plans in place, some rehearsals
1	Very Low	• Real options deployed to maximize strategic flexibility • High enterprise level/process level capabilities to address risks • Redundant response mechanisms in place and regularly tested for critical risks • Contingency and crisis management plans in place and rehearsed regularly

Illustrative Speed of Onset Scale		
Rating	**Descriptor**	**Definition**
5	Very High	• Very rapid onset, little or no warning, instantaneous
4	High	• Onset occurs in a matter of days to a few weeks
3	Medium	• Onset occurs in a matter of a few months
2	Low	• Onset occurs in a matter of several months
1	Very Low	• Very slow onset. occurs over a year or more

Source: Curtis and Carey, 2012.

If a particular risk is viewed as moderate, and yet this same moderate risk is magnified across various business units by cumulative effect, it may warrant raising the risk priority. Similarly, if a moderate risk is determined to have significant impact on additional risks, once again the re-prioritization of that risk may be justified. Another useful tool in this respect is scenario planning, which allows management to create, test, rehearse and refine strategies designed to be indicative of potential real-world events, through the use of narratives and story-telling. It can help answer questions such as "Which risks are likely to have the most significant impact" and "How will we know when the environment has changed" (Deloitte, 2019). It may be instrumental to redesign the risk response. Modifications to risk assessment results are indicative of a healthy and interactive process. Finally, risk assessments should be updated regularly, usually at least once per annum. Once the iterative process is complete, and top risks have been identified and prioritized, it is time to develop an appropriate response to such risks.

1.3.3. Risk response

One of the most useful tools in developing a response to a risk event is the bow-tie analysis (Figure 10). The bow-tie tool is designed to encourage ERM managers and professionals to look at both preventative measures (on the left side of the risk event "knot"), and reactive responses (on the right), towards a previously-identified top risk. It begins with an understanding of both the causes and the consequences of a risk event. To identify causes, it is important to pay

particular attention to the root causes, events and circumstances that might cause the risk event to occur. Once causality has been identified, the bow-tie analysis directs the organization to consider appropriate preventative measures to eliminate the risk altogether. In the event the organization determines it has little or no control over the risk event, the analysis shifts towards consequences, by asking what would those consequences be, and what mitigative measures might be undertaken to minimize the negative fallout.

▶Figure 10: Bow-tie analysis

Source: Hancock, n.d.

In determining an appropriate risk response, it is also important for an enterprise to take stock of its own appetite for risk. In 2009, the National Association of Corporate Directors (NACD) published a report that said, "a risk appetite statement resides at the heart of an effective risk management program and is linked to the organization's overall risk management philosophy and strategic ambition" (Quail, 2012). Similarly, the Office of the Superintendent of Financial Institutions of Canada (OSFI) has issued a guideline that says, "senior management should be able to identify and clearly articulate the institution's risk appetite and understand the impact of stress events on the risk profile of the institution." A well-defined risk appetite should be linked to the organization's strategic objectives and mission statement, and it should be expressed in such a way as to guide decision-makers to engage in intended behaviours and make appropriate choices in alignment with the organization's goals. However, this is in many instances easier said than done, and there remains little agreement as to how to define the risk appetite of an enterprise. For example, COSO's ERM framework defines it vaguely as "the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals." ISO 31000 conveniently side-steps the issue altogether, making no reference to the concept of risk tolerance or appetite (Quail, 2012). What then is risk appetite?

Risk appetite can be seen to encompass four fundamental areas: corporate values, strategy, stakeholders and capacity. Within the context of corporate values, an enterprise may ask of itself *What risks will we not accept?* Strategy addresses the question *What risks do we need to take?* Similar questions should be posited as to what risks stakeholders are likely to accept, and what capacity exists within the organization to absorb these risks. In a survey by PwC in 2013, 95% of respondent directors believed that their board had at least a moderate comprehension of their company's risk appetite, but they suggest that this might be of little value if this understanding is merely implicit and the company's approach to risk appetite is informal. Risk appetite should be more than just a policy statement; rather it should be viewed as an active and ongoing process, one that seeks to incorporate meaningful definitions of risk tolerance. Figure 11 provides an example as to how these definitions might be categorized. The risk appetite process can be described as having four components, assessing risk profile and risk

capacity, followed by a qualitative and quantitative risk assessment. This ties back to the analysis used to identify top risks, and the rankings of those risks in terms of priority (PwC, 2013).

Once an organization's risks have been identified and prioritized, and the enterprise's risk appetite has been defined, the business is well-positioned to determine an appropriate response to each risk. As previously alluded these responses can take one of four forms: avoidance, transfer, mitigation or acceptance. Avoidance is simply walking away from the risk altogether, for example selling a business unit, dropping a product line or exiting a geographic area. However, it is difficult to walk away from a business or a product line simply just based on future risk, and indeed it may be very costly to do so if previous investments have already been made. Risk transfer usually involves purchasing some degree of insurance, but as has been noted it is too costly to attempt to insure for every known risk.

There are however other ways to share risk. In financial enterprises this may include various hedging strategies to protect against contrary price movements in the market. Companies can also share risks and awards through joint venture agreements, a practice particularly common in the mining industry. The strategy is one of offsetting a portion of the identified risk, understanding that this will always entail a cost. Risk reduction or mitigation are also important valid risk responses in certain instances. For example, a company may seek to reduce its exposure in relying too heavily on one product by diversifying its product offerings, or it might split IT data centre operations into two different locations to reduce the risk of climate-related catastrophic failure. A final potential risk response is to do nothing at all. A company may look at the impact and likelihood of a risk and decide to simply accept the risk as is. Additionally, it might decide to self-insure, which while transferring risks from one area of the business to the whole of the enterprise is nevertheless itself a form of risk acceptance (Moeller, 2007).

▶Figure 11: Sample risk appetite scale

Risk Appetite Scale					
	Rating	**Philosophy** Overall risk-taking philosophy	**Tolerance for Uncertainly** Willingness to accept uncertain outcomes or period-to-period variation	**Choice** When faced with multiple options, willingness to select an option that puts objectives at risk	**Trade-off** Willingness to trade off against achievement of other objectives
5	**Open**	Will take justified risks	Fully anticipated	will choose option with highest return; accept possibility of failure	Willing
4	**Flexible**	Will take strongly justified risks	Expect some	Will choose to put at risk, but will manage impact	Willing under right conditions
3	**Cautions**	Preference for safe delivery	Limited	Will accept if limited, and heavily out-weighed by benefits	Prefer to avoid
2	**Minimalist**	Extremely conservative	Low	Will accept only if essential, and limited possibility/extent faillure	With extreme reluctance
1	**Averse**	"Sacred" avoidance of risk is a core objective	Extremely low	Will select the lowest rik option, always	Never

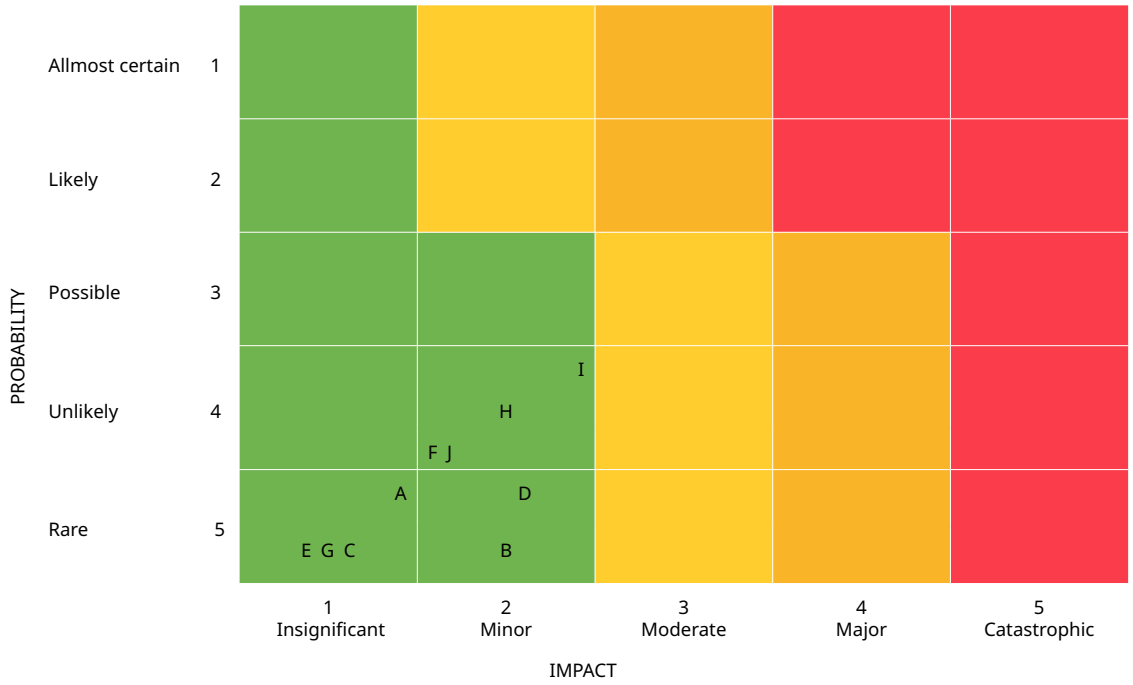
Source: Quail, 2012.

The final step in the process, prior to feeding back into the ERM ongoing process cycle is communication and monitoring. Effective risk reporting targeted towards the appropriate audience is a crucial last step in the first iteration of an ERM cycle. As a best practice, organizations should consider IT executives on their ERM steering committees with targeted reporting in mind. Without effective reporting all previous efforts are for naught. Reporting allows for the identification of escalating risks so that the enterprise is empowered to act upon those risks. The 2017 COSO ERM framework suggests that:

> "Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations"
>
> **(Williams,** 2018).

Risk reporting needs to consider the audience to which it is addressing the report. For larger enterprises this normally consists of four distinct groups: the board, or the board-level risk committee; senior management; the individual risk owners themselves; and, externally, the various regulatory authorities to which the enterprise is accountable (Williams, 2018). When reporting to the board it is imperative to strike the right balance. Reports to the board should be general (though substantive) in nature and not so specific as to bury board members in the minutiae of specific risk details. One way of accomplishing this is through the use of colour-coded heat maps, for example by graphing impact against likelihood as is depicted in Figure 12.

▶Figure 12: Colour-coding example for key risks



Source: Stern, 2016.

Senior management will have many of the same reporting requirements as the board, but they will also typically need to see a higher level of detail. This would normally entail assessments of impact, likelihood, vulnerability and velocity. An effective means of communicating this information is by way of a risk dashboard, a visual tool encompassing all of these factors, though once again customized to the specific needs of the organization. An example of a risk dashboard as developed the NC State ERM Initiative is presented in Figure 13, which provides information on key risks, the owners of those risks, risk status and rationale, and key management activities intended to respond to those risks. This is also where cumulative risks and interdependencies need to be addressed.

The last internal audience for risk reporting lies with middle management, who are the actual owners of individual key risks. This group requires the highest level of detail about risks in their own business units. These are the individuals who are responsible for implementing the risk responses prescribed by upper management. Reporting to this group should focus on key performance indicators (KPIs) and provide the most up-to-date information possible

▶Figure 13: Sample risk dashboard

Key Enterprise Risk	Risk Owner	Risk Status Q4 20xx (Prior Period)	Risk Status Q1 20xx (Current Period)	Risk Status Rationale	Key Risk Management Activities
Resource Optimization Risk Definition Inability to effectively allocate existing resources, and/or secure additional qualified resources, to enable IH to optimize business activities (operational and Strategic	JR			• Current resource capacity sufficient to execute current portfolio • Governance structure in place to manage prioritization of work • ERP Redesign implemented • Etc.	• Prioritization of strategic initiatives to set groundwork for resource optimization • Implemented ERP • Etc.
Medical Care Management Risk Definition Inability to maintain medical costs within a range that is consistent with forecasted patterns, optimizes competitive position, and achieves target	TF			• "Partnerships and Alignments" initiatives are on track • "Medical Expense Management" strategies in development, targets set; new initiatives underway to identify additional opportunities • Risk management effectiveness is also dependent upon constituent engagement (members, providers and physicians) • Etc.	• Development of Medical Management Annual Plan for 20XX • Medical Management initiatives underway to identify new opportunities • Etc.

Risk Status Key:

 **High**: risk management activities have not resulted in demonstrated improvement in the inherent risk exposure

 Medium: risk management activities have begun to demonstrate improvement in the

 Low: risk management activities have resulted in demonstrated improvement to adequately address of exceed inherent risk

Source: Williams, 2018.

Another important benefit of the bow-tie analysis is its ability to identify key risk indicators (KRIs). KRIs are critical predictors of potentially damaging risk events. They can serve as red flags, monitoring risk exposure and contributing to early warning signs of an impending risk event. KRIs are typically quantifiable and measurable. They are born out of high-quality data and are usually specific to a certain risk. KRIs form a key component on a typical risk dashboard, providing easily digestible colour-coded indications of an accelerating (or diminishing) risk profile over time.

Finally, many financial institutions and publicly traded companies are subject to regulatory oversight. The US Security and Exchange Commission requires risk disclosure for public companies, as does the state level Own Risk Solvency Assessment (ORSA) for insurance companies, or Solvency II reporting for insurance companies in the EU. It is therefore simply efficient and prudent to design internal reporting with these external considerations in mind.

1.4. Emerging ERM trends

Lawton (2022) summarizes the top ten ERM trends, based upon information published by Forrester Research:

1. *Risk maturity frameworks consolidate workflows*
   A risk maturity framework can be considered an ERM framework that has evolved continuously for some time, and is as up-to-date as is possible in terms of processes, technologies and information. It has all the best practices, as described in section 1.3 above, working seamlessly. Having achieved this level of maturity, it becomes clear that ERM not only serves to identify, assess and respond to risks, it actually connects the enterprise by consolidating workflows across disparate units within the business. This is achieved through communication and reporting, in a standardized form and lexicon common to all.

2. *ERM technology expands into governance risk and compliance (GRC)*
   As mentioned above, many enterprises are subject to varying degrees of regulatory oversight. ERM technology increasingly provides a means for consolidating information from across the enterprise into coherent regulatory reporting. It can help to identify gaps in compliance, provide guidance for management's response to risk, and automate the internal audit process. It can also be expanded into intelligence analytics for geopolitical risks, security systems for early detection of breaches of the network, and social media monitoring capabilities to detect changes in brand reputation.

3. *ERM is increasingly seen as a competitive advantage*
   A well-functioning ERM process not only identifies top risks to an organization, it can also reveal new opportunities along the way. An ERM process is about enhancing enterprise value; many enterprises are recognizing that instead of merely identifying, assessing and responding to risks, an effective ERM programme can actually serve as a competitive advantage. In the case of a systemic industry-wide, or even a global risk event, such as the COVID-19 pandemic, those companies with an ERM programme in place and having previously accounted for the risk are likely to face fewer disruptions to their operations, and lesser customer dissatisfaction in relation to their peers.

4. *Wider use of risk appetite statements*
   Risk appetite statements have been discussed at some length herein. Despite some of the challenges involved with articulating an effective risk appetite statement, one that does not dissuade the pursuit of new opportunities for example, or one that cannot be misinterpreted as condoning unacceptable levels of risk, risk appetite statements are rising in popularity. Senior executives in many organizations are coming to recognize that a well-composed risk appetite statement is integral to shaping the culture of risk within the enterprise, and in promoting appropriate behaviour.

5. *Panels of subject matter experts improve risk assessment and response*

This is an example of best practices in ERM coming to the fore. The previous section noted the need to bring together senior management and risk owners to challenge risk initial assessments through healthy debate, and to modify assessments accordingly. Enterprises are increasingly more cognizant of the need to integrate information in a useful format across the enterprise. Some organizations have been consolidating enterprise-wide risk information into their GRC platform, creating an informed network of subject matter for use across the whole of the organization.

6. *Risk mitigation and measurement tools multiply*
   Risk mitigation and measurement tools are becoming more integrated and more sophisticated in their approach. There now exists a wide array of third-party software vendors offering integrated ERM tools designed to present a holistic view of risks across the enterprise, to identify KRIs to show how a risk is trending, to promote accountability, and to provide real-time reporting to assist in decision making by senior management.

7. *Increase in scenario-planning and assumption-testing capability*
   In another example of ERM best practices becoming more mainstream, companies are increasingly turning to scenario planning, using simulations, war games, interactive workshops and the like. These exercises serve to promote cross-functional thinking about future risks, creating a more holistic view of the risk landscape, both internally and extrinsically.

8. *CIOs broker C-level buy-in*
   As referenced, some in senior management do not believe the benefits of a comprehensive ERM programme outweigh the costs. Chief information officers are progressively pushing the debate upwards through the organizational hierarchy, bridging the divide amongst C-suite executives to entrench risk and resilience plans within the upper echelons of the enterprise's power structure. CIOs are well-positioned in this respect, having access to information and by the fact that their responsibilities put them in contact with many different functional areas of the business.

9. *Cyber and physical risk coverage*
   In 2021, Russian hackers forced the shutdown of the Colonial Pipeline, the largest fuel pipeline in the US, and coopted a massive amount of data in a ransomware attack (Bloomberg, 2021). This is but one example amongst many where critical infrastructure is involved. Risks such as cyber-attacks can threaten the very existence of a business. Cyber threats are increasingly posing risks to physical infrastructure with both societal and business ramifications. Enterprises are recognizing the critical need to identify and plan for risks that may cut across both informational and physical boundaries.

10. *Integrating ERM with the digital transformation*
    Enterprises are recognizing that their legacy data systems are in many cases not well-equipped for handling the increasing complexity of the risk landscape. Some 75% of respondents to PwC's 2022 Global Digital Trust Insights Survey say that too much unnecessary informational complexity poses "concerning" cyber and privacy risks (PwC, 2022). Many enterprises find themselves dealing with runaway and befuddling complexity, where all too often individual technology solutions simply don't communicate with one another. C-suite leaders are recognizing this reality and are seeking to develop new cultural habits of coordination and collaboration, to both simplify and integrate IT solutions and outputs across all enterprise functions, and to merge them seamlessly into their GRC platforms. In this sense, ERM can be seen as a journey to maturity.

1.5. ERM challenges for SMEs

SMEs comprise most of the economic activity and employment globally, yet they face their own unique set of challenges, applicable to all aspects of their activities. This is particularly true in with respect to ERM programme development. One may reasonably ask the question that, given its inherent complexity, is ERM even suited to SMEs in the first place? This section will look at some of the challenges, encapsulated in three broad themes,

facing SMEs and whether or not ERM can really be a useful endeavour for smaller enterprises.

One of the biggest challenges facing SMEs is that of informational barriers and the knowledge gap which exist between high-income countries and developing countries. While informational barriers do exist for smaller enterprises in developed countries, the problem is much more acute in developing countries. In the case of SMEs, and especially for those in developing nations, these barriers are usually more pervasive, and more obstructive. In developing countries, the knowledge gap is often exacerbated by a lack of a strong underlying institutionalized education system. Public educational institutions are typically of poorer quality and inherently more fragile. Indeed, one of the fundamental problems is the dearth of any such risk-based skill sets in the first place. This translates directly to a scarcity of risk management expertise upon which to draw for many SMEs. SMEs are not likely to have in-house risk management resources or risk departments, risk committees and the like. Under such circumstances it is easy to imagine that the adoption of an ERM strategy might be seen as beyond all practical reach, if the SME is even aware of the concept in the first place. Embarking on an ERM programme is likely to involve entirely new skill sets, in both managerial and technical roles, a significant challenge for SMEs. Risk management-based skills development programmes are readily available in most western countries; however, this is not the usual situation in developing countries. Indeed, as far as such programmes do exist, progress is often impeded by a lack of awareness and poor communication with respect to their very availability.

A second critical impediment for SMEs is their relative lack of both human and financial resources. Contemplating risks far into the future is a luxury when the ongoing month-to-month or even week-to-week survival of the business may be top of mind. Competing priorities in a fragile business environment with thin margins are likely to push any thought of risk management, let alone ERM, to the back burner. As noted above, many senior managers of large corporations in the developed world still have a hard time reconciling diverting resources towards an ERM programme, failing to see any net strategic benefit to the organization. What then of the owners or managers of a small enterprise in an economically fragile business environment such as those typical of developing countries?

Finally, the risk responses available to SMEs, particularly in the developing world, are likely to be severely limited. Avoidance of risk altogether may be existential to the business, as some risk is inevitable and indeed necessary to the enterprise. The options for risk transfer may be scarce, expensive or indeed non-existent. Insurance may simply not be available, and other transference mechanisms, such as joint ventures may be out of reach to a small business whose networking opportunities may be severely limited. Mitigation efforts might be seen as too costly, leaving risk acceptance as the only option, leaving the survival of the business open to chance.

The fact that these challenges exist does not in any way diminish the value of embarking on an ERM programme. More than anything these impediments argue for external support in taking that next step to incorporating risk as part of the culture of the organization, regardless of its size. As noted, ERM is itself a necessarily customizable endeavour. There is nothing that says an ERM programme could not be tailored to a smaller enterprise. In certain instances, this might be accomplished by simply decreasing the level of complexity involved to be manageable within the context of a company's operational realities. Chapter 2 will explore this concept in greater detail.

1.6. Current risk management technologies and their impact on ERM

Historically, information technology was reactive in nature, putting out fires as they occurred, and dealing with necessary compliance issues. Later, IT served to proactively manage risk and compliance. Rasmussen and Stamp (2005) described a vision for the future, one in which ERM-based IT became a central nervous system of the organization, monitoring GRC thresholds across the enterprise in real time. Their vision of almost two decades ago has become a reality.

1.6.1. How technology drives ERM

As noted, ERM is increasingly seen by executives as an emerging core competency and competitive advantage. Meaningful data, provided at the right time and in an intuitive format that is easy to use, is essential for any successful ERM process. Data drives decision-making, but the output is only as good as the as the original data inputs. An effective ERM programme creates a central repository for information, but for many organizations there are significant challenges involved. As referenced herein, legacy IT systems are themselves often silo-based, and in many instances, they do not communicate well with one another, or indeed not at all. In such an environment, risk aggregation becomes near impossible. In fact the problem is so pervasive that the COSO 2017 ERM framework specifically references the critical dependency of information technology, and raises awareness of the problem, stating that:

> "When making investments in technology or other infrastructure, management (should) consider the tools required to enable enterprise risk management activities"
>
> **(Bayuk,** 2018).

Much like ERM itself, an enterprise's IT strategy is a process, one that is in a continuous state of flux as new and better technologies emerge. Enterprises are increasingly exploiting Big Data, analytics, cloud computing, enterprise resource planning (ERP), and GRC systems, all of which can serve to enhance risk management effectiveness (Patterson, 2015).

Information technology plays an important role in providing risk-related data in real time, and automating risk measurement and management processes, moving the organization towards greater risk awareness and control. Risk management fails when data is redundant, scattered and housed in separate silos. Successful risk management information architecture is able to integrate information from disparate business units and indeed external sources, and model risk causes and effects. A fully integrated technology platform can also serve to illustrate risk relationships across the entire enterprise. Real-time data drives heat maps, risk dashboards, predictive risk intelligence (PRI), and GRC platforms. Some of the largest multinational organizations are moving towards a centrally managed enterprise risk centre (ERC). An ERC effectively harnesses technology to consolidate all ERM functions into a single risk operations centre, combining network and cyber security functions with physical security monitoring, financial operations, customer service, and any such other areas of potential key risks as identified by the organization.

Data in and of itself is not inherently useful, it needs to have context and communicate a clear and actionable message. An effective IT platform enables collaboration and brings order to key interdepartmental processes, and in so doing can reveal important risk interdependencies across the enterprise. When a risk crosses a predetermined threshold, automated alerts can allow for faster and more effective responses. The right person can be notified and prompted to act, and risk owners can have a better view of their portfolio and prioritize actions accordingly. For SMEs, there is an abundance of commercially available "off the shelf" ERM and GRC software that can provide this functionality. The importance of communication and monitoring has been well-documented herein. ERM technology, when coupled with advanced analytics, can simplify reporting that is customizable to the target audience, such as

heat maps for the board, dashboards for senior management and granular reports for risk owners on the front line. It can offer greater visibility of the performance of an ERM programme, thereby proving the value of ERM to those who might have otherwise harboured some doubts.

Some of the core IT capabilities to ensure an effective ERM program include:

- Internal integration across the enterprise
- Content, workflow and task management
- 360° contextual awareness in GRC
- Support for multiple risk frameworks
- Definition of objectives and controls for risk
- Ability to effectively establish and communicate risk policy
- Management of incidents and losses
- Allocation of risk responsibility
- Effective reporting and trend analysis
- Analytics and modelling capabilities such as scenario planning
- Identification of risk interdependencies

Source: Rasmussen, 2018.

1.6.2. Types of risk management technologies

The value of real-time automated processes, the generation of heat maps and risk dashboards and the like have been detailed. However there are new and emerging technologies that promise to radically alter the ERM process; indeed they have already begun to do so. Artificial intelligence (AI), where computers are able to ingest and organize massive amounts of data, and then employ algorithms to self-learn and apply logical thinking to a problem is in its infancy, but it is here nevertheless, and it has enormous implications for ERM. AI will increasingly provide risk managers the ability to capture, extract and transform data from legacy databases, allowing them to perform risk assessments, stress tests and risk scenario analyses (Patterson, 2015). Impossible until recently, automated ERM processes can now gather real-time data from external sources such as Thompson Reuters, Bloomberg, the Wall Street Journal and the like, and seamlessly integrate them into automated ERM analysis. Some cutting-edge IT tools engage agency software to "crawl" across the internet, social media sites, or an organization's Big Data warehouses to collect emerging risk-related intelligence (Patterson, 2015).

Deloitte (n.d.) points to predictive risk intelligence (PRI) as a key component of an organization's ability to keep ahead of emerging risks. They describe predictive risk analytics as identifying the key drivers of a risk, employing scenario analysis, determining probabilities, calculating risk values, and defining accountabilities. Technology has a crucial role to play in this respect. Robotics process automation (RPI) can collect data on a real-time basis, and is able to integrate unstructured and nonlinear data relationships into a coherent message. The agency software described above is a pertinent example of RPI. RPI uses character recognition and language processing capabilities and employs cognitive intelligence to assimilate vast amounts of data from both internal and exogenous sources, and then standardizes and aggregates that data into a form suitable for predictive modelling techniques. AI and machine learning work to put that data to use in predictive risk modelling and analysis. Based upon identified risks, analytical models are employed to interpret outcomes and generate PRI. This too is an ongoing process, as the models may be changed or updated depending upon the evolving risk landscape, or indeed upon the PRI that is generated by those same models. Finally, as referenced above, technology allows for the development of an appropriate response and for effective communication through automated remediation and reporting.

The next generation of cognitive computing and machine learning applications, along with advances in natural language programming are likely to radically transform ERM processes, allowing users to connect, correlate and utilize information in ways never imagined.

▶Appendix 1: Global risks 2022

	Global Risk	Description
Economic	**Asset bubble bursts** in large economies	Prices for housing, investment funds, shares and other assets in a large economy increasingly disconnect from the real economy
	Collapse of a systemically important industry	Collapse of a systemically important global industry or firm with an impact on the global economy, financial markets and/or society
	Debt crises in large economies	Corporate and/or public finances overwhelmed by debt accumulation and/or debt servicing in large economies, resulting in mass bankruptcies. defaults, insolvency, liquidity crises or sovereign debt crises
	Failure to **stabilize price** trajectories	Inability to control an unmanageable increase (inflation) or decrease (deflation) In the general price level of goods and services
	Proliferation of **illicit economic activity**	Global proliferation of informal and/or illegal activities that undermine economic advancement and growth: counterfeiting, illicit financial flows, illicit trade, tax evasion, human trafficking, organized crime etc.
	Prolonged economic **stagnation**	Near-zero or slow global growth lasting for many years
	Severe **commodity shocks**	Abrupt shocks to the supply and demand of systemically important commodities at a global scale that strain corporate. public and/or household budgets: chemicals, emissions, energy, foods, metals, minerals etc.
Environmental	**Asset bubble bursts** in large economies	Prices for housing, investment funds, shares and other assets in a large economy increasingly disconnect from the real economy
	Collapse of a systemically important industry	Collapse of a systemically important global industry or firm with an impact on the global economy, financial markets and/or society
	Debt crises in large economies	Corporate and/or public finances overwhelmed by debt accumulation and/or debt servicing in large economies, resulting in mass bankruptcies. defaults, insolvency, liquidity crises or sovereign debt crises
	Failure to **stabilize price** trajectories	Inability to control an unmanageable increase (inflation) or decrease (deflation) In the general price level of goods and services
	Proliferation of **illicit economic activity**	Global proliferation of informal and/or illegal activities that undermine economic advancement and growth: counterfeiting, illicit financial flows, illicit trade, tax evasion, human trafficking, organized crime etc.
	Prolonged economic **stagnation**	Near-zero or slow global growth lasting for many years
	Severe **commodity shocks**	Abrupt shocks to the supply and demand of systemically important commodities at a global scale that strain corporate. public and/or household budgets: chemicals, emissions, energy, foods, metals, minerals etc.
Geopolitical	**Collapse** of a **multilateral** institution	Dissolution of a global multilateral institution established to resolve economic, environmental, geopolitical and/or humanitarian crises with regional or global implications: border disputes, environmental commitments, migration crises, health emergencies, trade disputes etc.
	Fracture of **interstate relations**	Economic, political and/or technological rivalries between geopolitical powers resulting in a fracture of bilateral relations and/or growing tensions
	Geoeconomic confrontations	Deployment of economic levers. including investment controls, trade controls. non-tariff barriers and/or currency measures, by global or regional powers to decouple economic interactions between nations and consolidate spheres of influence
	Geopolitical contestation of strategic **resources**	Concentration. exploitation and/or mobility restriction by a state of goods, knowledge, services or technology critical to human development with the Intent of gaining geopolitical advantage
	Interstate conflict	Belligerent bilateral or multilateral conflict between states with global consequences: biological, chemical, cyber and/or physical attacks, military interventions, proxy wars etc.
	State collapse	Collapse of a state with global geopolitical importance as a result of internal conflict, breakdown of rule of law, erosion of institutions, military coup, regional or global instability
	Terrorist attacks	Large-scale, scattered or isolated terrorist attacks carried out by individuals or non-state groups with ideological, political or religious goals, resulting in loss of life, severe injury and/or material damage
	Weapon of mass destruction	Deployment of biological, chemical, cyber, nuclear or radiological weapons, resulting in loss of life, destruction and/or international crises

Societal	**Collapse** or lack of **social security** systems	Non-existence or widespread bankruptcy of social security systems and/or erosion of social security benefits: disability, elder1y, family, injury, maternity, medical care, sickness, survivor, unemployment etc.
	Employment and **livelihood crises**	Structural deterioration of work prospects and/or standards for the working-age population: unemployment, underemployment lower wages, fragile contract$, erosion of worker rights etc.
	Erosion of **social cohesio**n	Loss of social capital and a fracture of social networks negatively impacting social stability, individual well-being and economic productivity as a result of persistent public anger, distrust, divisiveness, lack of empathy, marginalization of minorities, political polarization etc.
	Failure of **public infrastructure**	Unequitable and/or insufficient public infrastructure and services as a result of mismanaged urban sprawl, poor planning and/or under-investment, negatively Impacting economic advancement, education, housing, pubic health, social inclusion and the environment
	Infections diseases	Massive and rapid spread of viruses, parasites, fungi or bacteria that cause an uncontrolled contagion of infectious diseases, resulting in an epidemic or pandemic with loss of life and economic disruption
	Large-scale **involuntary migration**	Large-scale involuntary migration induced by climate change, discrimination, lack of economic advancement opportunities, persecution, natural or human-made disasters, violent conflict etc.
	Pervasive **backlash against science**	Censure. denial and/or scepticism towards scientific evidence and the scientific community at a global scale, resulting in a regression or stalling of progress on climate action, human health and/or technological innovation
	Pollution-driven **harms to human health**	Physical and mental health impacts from harmful chemical or other particulates in the air, water or food, which may stem from energy generation, industrial and agricultural practices, waste management failures, natural disasters, human behaviour and other sources
	Severe **mental health deterioration**	Pervasiveness of mental health ailments and/or disorders globally and across multiple demographics, negatively impacting well-being, social cohesion and productivity: anxiety, dementia, depression, loneliness, stress etc.
Technological	**Adverse** outcomes of **technological advances**	Intended or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing etc.
	Breakdown of critical information **infrastructure**	Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites etc.
	Digital inequality	Fractured and/or unequal access to critical digital networks and technology, between and within countries, as a result of unequal investment capabilities, lack of necessary skills in the workforce, insufficient purchase power, government restrictions and/or cultural differences
	Digital power concentration	Concentration of critical digital assets, capabilities and/or knowledge by a reduced number of individuals, businesses or states. Resulting in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access etc.
	Failure of **cybersecurity** measures	Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by Increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability
	Failure of **technology governance**	Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards

Source: WEF, 2022.

▶Appendix 2: Comparison of COSO frameworks to ISO Annex SL

Clause	Annex SL heading	COSO ERM cube (2004)	COSO framework 2017
4.	**Context of the organization**		
4.1	Understanding the organization and its context	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholders expectations Component 3: Event Identification includes internal and external events that could have positive or negative impact on objectives	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy& Objective-Setting includes context, risk appetite and setting of strategy and business objectives
4.2	Understanding the needs and expectations of stakeholders		
4.3	Determining the scope of the management system		
4.4	The management system		
5.	**Leadership**		
5.1	Leadership and commitment	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities
5.2	Policy		
5.3	Organisational roles, responsibilities and authorities		
6.	**Planning**		
6.1	Actions to address risk and opportunities	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholders expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy& Objective-Setting includes context, risk appetite and setting of strategy and business objectives
6,2	Management system objectives and planning to achieve them		
7.	**Support**		
7.1	Resources	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholders expectations Component 7: Information & communication includes need for relevant quality information to be captured and communicated	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 5: Information, Communication & Reporting includes communication, use and reporting of risk information
7.2	Competence		
7.3	Awareness		
7.4	Communication		
7.5	Documented information		
8.	**Operation**		
8.1	Operational planning and control	Component 4: Risk Assessment includes determination of impact, likelihood and inter-relationships of risks Component 5: Risk Response includes actions to align portfolio of risks with risk tolerance and risk appetite	Component 3: Performance includes risk identification ans assessment, risk response and inter-relationship o risks
9.	**Performance evaluation**		
9.1	Monitoring measurement, analysis and evaluation	Component 6: Control Activities includes actions to ensure risk responses are effective and efficient Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
9.2	Internal audit		
9,3	Management review		
10.	**Improvement**		
10.1	Non-conformity and corrective actions	Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
10.2	Continual improvement		

Source: IRM, n.d.

References

American Physical Society, 2009. July 1654: Pascal's Letters to Fermat on the. [online] Aps.org. Available at: <https://www.aps.org/publications/apsnews/200907/physicshistory.cfm> [Accessed 2 May 2022].

Bayuk, J., 2018. Technology's Role in Enterprise Risk Management | ISACA Journal. [online] ISACA. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/technologys-role-in-enterprise-risk-management> [Accessed 22 May 2022].

Beasley, M., 2020. What is Enterprise Risk Management (ERM)? | ERM - Enterprise Risk Management Initiative | NC State Poole College of Management. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/library/article/what-is-enterprise-risk-management> [Accessed 2 May 2022].

Bloomberg, 2021. Hackers Breached Colonial Pipeline Using Compromised Password. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password> [Accessed 21 May 2022].

Branson, B., Beasley, M. and Hancock, B., 2019. 2019 The State of Risk Oversight AN OVERVIEW OF ENTERPRISE RISK MANAGEMENT PRACTICES. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_Risk_Oversight.pdf> [Accessed 12 May 2022].

Claypole, A., 2021. The COSO ERM framework explained | Ideagen. [online] Ideagen.com. Available at: <https://www.ideagen.com/thought-leadership/blog/the-coso-erm-framework-explained> [Accessed 2 May 2022].

Curtis, P. and Carey, M., 2012. Risk Assessment in Practice. [online] Www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf> [Accessed 17 May 2022].

Deloitte, 2019. Scenario planning and war-gaming: Sizing up the future. [online] Www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-reimagining-rie-eminence-series.pdf> [Accessed 18 May 2022].

Deloitte, n.d. Seeing the Storm Ahead: Predictive Risk Intelligence. [online] Www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-seeing-the-storm-ahead.pdf> [Accessed 2 May 2022].

Hancock, B., n.d. The bow-tie analysis: a multipurpose erm tool. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/az/erm/i/chan/library/The_Bow-Tie_Analysis-_A_Multipurpose_ERM_Tool.pdf> [Accessed 14 May 2022].

ILO, 2020. Driving Up Productivity GUIDE FOR EMPLOYER AND BUSINESS MEMBERSHIP ORGANIZATIONS. [online] Ilo.org. Available at: <https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---act_emp/documents/publication/wcms_758749.pdf> [Accessed 16 May 2022].

Martens, F. and Rittenburg, L., 2020. RISK APPETITE– CRITICAL TO SUCCESS USING RISK APPETITE TO THRIVE IN A CHANGING WORLD. [online] Coso.org. Available at: <https://www.coso.org/Shared%20Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf> [Accessed 19 May 2022].

Metricstream, n.d. The Power of Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM). [online] Metricstream. Available at: <https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm> [Accessed 18 May 2022].

Moeller, R., 2007. COSO enterprise risk management. 2nd ed. Hoboken, N.J.: John Wiley & Sons, pp.74 -75.

NC State ERM Initiative, 2020. ISO's Risk Management Framework | ERM - Enterprise Risk Management Initiative | NC State Poole College of Management. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/library/article/isos-risk-management-framework> [Accessed 24 April 2022].

NC State ERM Initiative, 2020. ISO's Risk Management Framework | ERM - Enterprise Risk Management Initiative | NC State Poole College of Management. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/library/article/isos-risk-management-framework> [Accessed 19 May 2022].

NC State ERM Initiative, 2022. Executive Perspectives on Top Risks. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/az/erm/i/chan/library/2022-executives-top-risks-report.pdf> [Accessed 11 May 2022].

Patterson, T., 2015. The Use of Information Technology in Risk Management. [online] Us.aicpa.org. Available at: <https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/asec_whitepapers/risk_technology.pdf> [Accessed 22 May 2022].

PwC, 2022. 2022 Global Digital Trust Insights Survey. [online] pwc.com. Available at: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html?#content-free-1-be77> [Accessed 20 May 2022].

Rasmussen, M. and Stamp, P., 2005. IT's Role in Enterprise Risk Management. [online] CSO Online. Available at: <https://www.csoonline.com/article/2118127/it-s-role-in-enterprise-risk-management.html> [Accessed 22 May 2022].

Rasmussen, M., 2018. How Technology Enables Enterprise Risk Management. [online] DoubleCheck Software. Available at: <https://www.doublechecksoftware.com/how-technology-enables-enterprise-risk-management/> [Accessed 22 May 2022].

Rhodes, A., n.d. A Brief Summary of the Long History of Risk Management. [online] Ventivtech.com. Available at: <https://www.ventivtech.com/blog/a-brief-summary-of-the-long-history-of-risk-management> [Accessed 2 May 2022].

Schmitt, J., Salvai, P. and De Koster, A., 2021. Membership Strategies and Policies:. [online] Itcilo.org. Available at: <https://www.itcilo.org/sites/default/files/2021-07/Membership%20Manual%20FINAL_web.pdf> [Accessed 15 May 2022].

Stern, C., 2016. ERM - Key Risk Indicators article. [online] First Consulting. Available at: <https://www.firstconsulting.com/articles/erm-key-risk-indicators-article> [Accessed 18 May 2022].

Ten Six Consulting, 2018. What Risk Management Technology Should You Use?. [online] Ten Six Consulting. Available at: <https://tensix.com/what-risk-management-technology-should-you-use/> [Accessed 2 May 2022].

WEF, 2021. The Global Risks Report 2021. [online] Www3.weforum.org. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf> [Accessed 2 May 2022].

WEF, 2022. The Global Risks Report 2022. [online] Www3.weforum.org. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf> [Accessed 2 May 2022].

Williams, C., 2018. The Ultimate Primer for Effective Risk Reporting. [online] Carol Williams. Available at: <https://www.erminsightsbycarol.com/risk-reporting/> [Accessed 19 May 2022].

UN Women. 2017a. Making Gender-responsive Migration Laws, Policy Brief No. 4. New York. Available

2

What EBMOs can do to support member enterprises in fostering business productivity and resilience through ERM

2.1. The strategic value of EBMOs

EBMOs serve two distinct but equally important roles for their members. The first role is that of advocacy, providing a collective voice for their constituents. Advocacy through EBMOs provides a forum in which smaller member organizations can have a seat at the table and express their own points of view, in a manner in which might not otherwise be possible. EBMOs will often have a wealth of knowledge with respect to their industry sectors, often more so than the policy makers themselves, and in fact they can serve to educate policy makers in advance of the adoption of any new policy or regulatory change. This can be a positive feedback loop, whereby policy makers are educated by industry experts, making their own jobs more productive, while all stakeholders benefit from the resultant informed and coherent policies themselves. Within this process EBMOs can develop better relationships with their governmental contacts, which can serve to smooth the way to address additional issues as they arise in the future. The advocacy role is often what attracts new members to business and industry associations in the first place. However, advocacy alone is not sufficient in and of itself to maintain a robust and engaged membership base over time.

The second primary role of EBMOs is to provide services to its members. Companies around the world in all sizes and various sectors consult associations for expertise on critical issues related to sustainable development and corporate citizenship. To strengthen industry reputation and competitiveness, these associations engage in a range of activities that advance their members' corporate sustainability practices. With the appropriate focus at the strategic level, the same can hold true for risk management practices, as one component of overall corporate sustainability. This is important as not all members are motivated to pay membership dues simply for an advocacy function, since the benefits of successful policy outcomes tend to create spill-over effects to the benefit of members and non-members alike. To retain membership, EBMOs must provide real and ongoing value-added to its membership base, and they must be able to adapt to changing circumstances to remain relevant. This flexibility requires a well-designed organizational hierarchy and strong board level governance, a hallmark of the largest and most successful EBMOs. However, and while adaptability is important, EBMOs must also have a clearly defined vision and mission both in terms of advocacy and in the provision of services if they are to be effective on behalf of their constituents. This represents a fundamental opportunity in ERM: by recognizing and fostering productivity and resilience amongst their members, and by embedding these concepts into their strategic objectives and mission statements, EBMOs can have a profound impact across differing industry sectors. EBMOs who support best practices in ERM can work with members to educate them as to the benefits and existent opportunities in a holistic and enterprise-wide approach towards risk management. SMEs may not even be aware of the benefits of an effective ERM programme, or may feel it is too costly, that they do not have sufficient managerial resources, or that there are more important priorities competing for attention. EBMOs can also assist in the development of progressive ERM programmes tailored to the needs of individual members, regardless of their size, and in doing so to promote productivity and resilience along the way, with the net effect of enhancing overall enterprise value.

2.2. Existing tools and services of EBMOs

EBMOs have a wealth of tools at their disposal in pursuit of their respective organizational missions. Once again, the tools employed by EBMOs can be viewed through the lens of their advocacy role, as well as by looking at specific services that provide value to the membership group. Not only do EBMOs lobby for improved regulatory environments, incentives towards enterprises to invest and generally to seek more favourable policy outcomes, they can also act as consultants to governments, at national, regional, and local levels. A well-functioning EBMO will have a wealth of sector-specific industry information and will generally include industry leaders and experts, whose goals in most cases are to work towards developing a productive and resilient industry sector. This can be accomplished by offering sector-specific advice, developing applicable tools,

and promoting best practices. This can apply to all aspects of an EBMO's strategic objectives and mission, but it can also pertain specifically to the creation of comprehensive risk management strategies amongst its constituent members, and to the development of effective ERM programmes.

The bringing together of industry leaders to tackle sectoral issues is itself a key service provided by EBMOs on behalf of their membership, creating an environment in which SMEs may benefit from the efforts of their larger counterparts. This is also true in risk management. In this sense a strong industry association can play the role of consultant to government as part of an integrated policy approach involving all stakeholders in recognizing a need for comprehensive risk management policy. In a healthy tripartite relationship (i.e. involving governments, EBMOs and member enterprises), governments may in some cases actively seek out the advice of EBMOs prior to implementing changes in risk policy. As referenced, and in the best-case scenarios a positive feedback loop can be created where EBMOs channel feedback and disseminate information back to their constituents, creating a positive environment for the successful implementation of beneficial regulation and policy. In addition to direct lobbying, there exist other tools at the disposal of EBMOs to influence the risk policy-making process, including the use of dialogue platforms, grassroots campaigns, and public relations initiatives (Mikhnev, 2006).

The delivery of regular value-added services to members is foundational to the value proposition of EBMOs and is the key to their staying relevant. Without such services membership and participation rates are likely to wane to the point of undermining the very existence of the EBMO. There exists a wide range of tactics that EBMOs can employ to directly engage the membership base. While some of these approaches represent relatively generic traditional EBMO services offerings to members, they can be equally viewed through an ERM-centric lens:

1. *Advising members of new third-party ERM products and services and actively working with members to implement them.*

There are an ever-increasing number of third-party tools for ERM available off the shelf, and these can range from the relatively basic to highly complex tools designed to help identify risks, assess their impact, likelihood, the enterprise's vulnerability to said risks, as well as their potential speed of onset of a negative or disruptive event. Actual risk response is highly specific to a business and is dependent upon intrinsic issues such as risk appetite and the resources, both human and financial, that are available within the organization. However, when it comes to communication and monitoring, tools designed to standardize reporting, create heat maps and risk dashboards and the like are all readily available in the private marketplace. EBMOs can provide a useful service to their members by proactively assessing and ranking the efficacy of the complex range of products available in this respect, and by providing bulletins to members as to what it might be recommended based upon best practices, the quality and uptake of a particular product amongst other members, and the level of sophistication or training required to ensure maximum benefits are derived from these products.

EBMOs can go a step further and become expert in various products that are available in the marketplace and position themselves to assist in their implementation and usage. In lieu of developing in-house expertise, there is little doubt that an opportunity exists to create partnerships with previously identified third-party vendors, to promote those vendors within the constituent base, in a mutually beneficial and symbiotic relationship. This may include an initiative whereby contact information of members is provided to exogenous private suppliers of ERM tools (with members' prior consent, as may be divulged in privacy policy, terms of engagement or some other mechanism defining the EBMO-member relationship), thereby effectively supercharging the sales efforts of these vendors. When combined with the EBMO's efforts in furtherance of ERM practices amongst its membership group, there is likely to be greater uptake in these products resulting in improved risk practices. This may in turn spur additional thought and consideration of adopting more comprehensive ERM practices

within individual member organizations. For those often-smaller companies that do come to see the value inherent in third-party ERM off-the-shelf offerings, without having to dedicate scarce resources to reinvent the wheel, there is likely to be a greater uptake in progressive risk management practices within their own organizations generally. The net result: enhanced corporate resilience and an increase in overall enterprise value.

2. *Hosting industry events that bring together industry leaders to allow for networking and relationship building.*

Industry events are generally designed to bring together a host of industry leaders, experts and other participants, allowing for discussion and collaboration in areas of common interest to the overall benefit of their specific industry sector. Such networking opportunities also provide important operational leverage for smaller industry participants to share in the hard-earned knowledge and expertise of their larger counterparts. This can be true for all aspects of an industry, but such events can also be tailored specifically with an ERM-centric focus. The goal in such high-level events would not necessarily be to discuss the specifics of an ERM programme, but rather to raise awareness of the value and importance of ERM in general, all while providing a valuable networking occasion as an incentive for member participants. Such events can also provide the opportunity for smaller member organizations, those that are less likely to have a mature ERM programme in place, to speak and engage with their larger counterparts on the issue, leveraging the experience of those who are much more likely to have some sort of ERM process already embedded within their own enterprise strategy and culture.

3. *Providing industry-wide and sector-specific market information to members.*

EBMOs can provide an extremely valuable service in terms of sector-specific data collection and data analytics. This is especially true with respect to ERM. The opportunity exists to custom design specific survey templates for the membership base on the issue of ERM, and then to engage members with those surveys. The resultant data would provide the basis for analytics, benchmarking, and the identification of surface trends, all of which might constitute invaluable information for individual members in terms of developing actionable responses to risk events. This in turn would allow for more effective strategic and risk planning, and ultimately result in an improved business climate overall. EBMOs who are inclined towards a focus on holistic risk management can take this a step further. While an ERM programme is necessarily specific to the organization, there is no reason why an EBMO could not conduct a broad sector-specific exogenous risk inventory on its own, and then conduct its own assessment of these extrinsic risks, including their impact, likelihood, vulnerability, and velocity, that can then be shared with its constituents. While this is by no means the totality of the necessary analysis, it is a good start. This information could prove to be of considerable value to an EBMO's constituent base, especially for smaller member organizations who might be struggling with the adoption of their own ERM programme, due to limited resources, experience and competing priorities. Naturally developing a risk response and a communication and monitoring programme is well outside the purview of an EBMO and is entirely specific to the individual enterprise in question. For those constituent SMEs that are perhaps somewhat more reliant on legacy-based risk management methods, this resultant insight might prove invaluable in the identification of external risks that might otherwise have fallen between the individual silos of a more traditional risk management approach.

4. *Engaging members with seminars, conferences, and training and development sessions.*

Among the most essential services that EBMOs can impart to their members is that of providing seminars, workshops, conferences, and hands-on skills development training initiatives. For those EBMOs that have adopted ERM as core to their central strategic mission, the next logical step is to work to educate their membership base in the inherent value of the

approach. In contrast to networking events and the like, it is in this capacity that EBMOs can become more targeted in their efforts to assist their members in developing the core competencies required for the successful implementation of an ERM programme. Such training can drill down into virtually all the key elements of the ERM programme development as described extensively in Chapter 1. This may include everything, from the broad identification of a risk inventory to the assessment and prioritization of risks, to developing responses and constructing effective communicating and monitoring procedures. Such programmes can delve even deeper into tools and approaches necessary to identify and implement these broad constructs. These may include courses on risk assessment, including such elements as risk ranking or scoring, or defining the risk appetite of the organization. It may include technology courses related to communication or monitoring tools such as heat maps, risk dashboards and the like. An EBMO which is intent on furthering ERM amongst its constituents might be well-advised to review these best practices in ERM programme development, and then devise its own systematic course structure considering an effective ERM approach in a manner tailored to its own sectoral realities.

5. *Improving awareness of existing support programmes upon which members may be able to capitalize.*

The COSO 2017 ERM framework and the ISO 31000:2018 framework have been referenced in detail in Chapter 1. These frameworks represent important resources upon which companies can draw in attempting to initiate or improve an ERM programme. EBMOs are well placed to interface between the COSO and ISO organizations and frameworks, and their membership base. They can serve to facilitate introductions and communication between these framework organizations and their member constituents. COSO and ISO can themselves benefit from increased visibility and the potential for additional adoption of their services; enterprises can benefit by adhering to a state-of-the-art ERM approach, which ultimately results in the end goal of enhanced enterprise value. The EBMO in its intermediary role can gain additional recognition and credibility through COSO and ISO, while also delivering an important value-added service to its members, and in so doing strengthen its own organizational resilience to better execute its strategic mission.

Succinctly put, EBMOs can fulfil a valuable role in seeking out exactly what programs may exist, be they public or private, that might be of specific value to their industry sector, and to communicate the existence of these resources to their members who heretofore may have been either unaware of their existence or preoccupied with other priorities.

6. *Improving corporate reputations through public awareness campaigns.*

Increasingly enterprises, large and small alike, identify potential damage to the organization's corporate reputation because of extrinsic forces is seen as a leading risk factor (NC State ERM Initiative, 2022). An enterprise's corporate reputation can take years, even decades to build, and as such it represents a valuable asset that must be protected and indeed nurtured. An enterprise's approach towards risk, particularly in areas which have the potential to impact the greater public good such as energy, water, and other critical infrastructure, can be highly determinate in securing its corporate reputation. One misstep can undo years of accumulated goodwill. EBMOs can do much to support and enhance the good reputation of its members by conducting public awareness campaigns which emphasize their members' proactive and state-of-the-art approach to risk management as a responsible strategy aimed at enhancing the public good and promoting benefits to society at large. At the same time, they can promote awareness of their industry sector's contribution to the overall benefit of society, demonstrating that there can exist positive interdependencies when speaking of risk management in terms of enhancing enterprise value. In addition, consumers, employees, and other stakeholders are also increasingly demanding sustainable practices on the part of the companies with whom they interact. Sustainability inherently includes resiliency,

whether towards climate shocks or any other risks, and as has been discussed, a coherent and effective risk management strategy is a key component towards enhancing resiliency. As Jain, Hagenbeek and Shogren (2021) point out, "Sustainability is in demand." Companies must continue to transform their enterprises and innovate to stay relevant to a consumer base in which sustainability is increasingly top of mind. The same holds true for employees and other stakeholders, with employees demanding sustainability on the part of their employers, and investors increasingly factoring in sustainability as an investment criterion.

7. *Developing industry and technical standards.*

An important value proposition of EBMOs is their ability to collect and aggregate data across their sectors, and in some instances to work with regulators to develop industry and technical standards to provide a baseline that members might eventually adopt and adhere to. This can allow for benchmarking and effective data tracking on corporate practices, which in turn can drive better decision making at the enterprise level. This is often the case with safety protocols and climate change mitigation for example, but the opportunity exists to apply similar frameworks with a view towards holistic risk management. This may include the design of sector-specific surveys and templates to facilitate effective ERM programmes across the membership base, particularly for smaller enterprises who once again may feel that their resources are already stretched to the limit. Pre-defined surveys for example may be useful in helping member enterprises in establishing a risk inventory, while certain other templates might be helpful in promoting effective communication and monitoring of an ERM process. These might include such previously discussed tools as heat maps, risk dashboards and the like that serve to ensure management is constantly aware of the ever-shifting risk landscape and of any individual risks that might be accelerating towards a disruptive event.

8. *Providing consulting services to individual members.*

Another important value-added service that EBMOs can provide to their members is that of offering consultancy and advisory services tailored specifically to the needs of individual member organizations. Consulting services can be applied towards any number of areas of key strategic importance to the organization, not the least of which is ERM. Indeed, in the event the EBMO in question has already made the determination that support for ERM practices amongst its constituents should in fact be a part of its strategic goals and core mission, it would be inherently well-positioned to proactively market such services to its members. Not would this be beneficial to its membership base, it would allow for additional and personalized interaction between the EBMO and its members, and in doing so enhance the EBMO's own revenue, productivity, and resilience along the way.

To be effective, the services referenced above must consider a long-term vision based on adaptive planning and strategic foresight. EBMOs must be flexible and responsive enough to respond to a rapidly changing business environment and an evolving risks landscape, and to incorporate forward-looking ERM thinking into the development of future services for their members. In measuring EBMOs' success, communicating a coherent vision and having strong governance and organizational structures are at the core. Without clear communication of strategic goals and a strong foundation it is unlikely that any of the above approaches would be successful in achieving the desired outcomes.

2.3. EBMOs and ERM: In the trenches

Much like the members they serve, EBMOs must have a clearly articulated mission statement reflecting their core values and their very reason for being. As referenced in Chapter 1, the business environment is becoming ever more complex, and the risk landscape is forever evolving. So too then the mission statements and core strategy of EBMOs must be periodically reviewed, and sometimes modified, for EBMOs to stay relevant to their members. This is especially true with respect to the potentially existential threats posed by climate change, economic crises, disease, and geopolitical conflicts. EBMOs must first determine whether they are ready to promote and engage with members on the issue of holistic risk management as part of their core mission. Increasingly this is the case, as customers, investors, governments, employees, suppliers, and indeed all stakeholders raise their collective voice to demand that effective risk policies and practices are in place to protect the interests of everyone concerned.

One avenue an EBMO might consider is re-branding itself as an entity dedicated to enhancing productivity and resilience within its constituent base, with a specific emphasis on a holistic approach towards risk management. Re-branding is much more than a new logo; a good brand tells members what their EBMO stands for, and ideally leaves a strong impression. A successful re-brand makes the EBMO stand out, and creates greater recognition, which can in turn lead to new member subscriptions and new possibilities for EBMOs to engage in robust ERM with those new members in what amounts to a virtuous circle. Re-branding with a focus on members' productivity and resilience must be backed up by actions however, lest the EBMO run the risk of reputational damage by failing to follow through on its stated mission.

A practical way in which EBMOs might support their members in ERM programme efforts is to appoint an individual to be the focal point to deal with issues specific to risk management. This might entail creating the position of ERM manager or a dedicated subcommittee within the organizational structure of the EBMO. The ERM manager would likely be tasked with creating a comprehensive strategy across the membership base, with a goal of improving resiliency within the entire industry sector, or with providing technical advice to members interested in developing a tailor-made risk management strategy for their enterprises. This might help to prepare members for emerging or escalating risks and black swan-style events. The ERM manager could create pragmatic feedback pertaining to on-the-ground realities to the General Director and the governance group, such that the strategic objectives and the mission statement of the EBMO can be reviewed and modified if so warranted. This might include identifying the practical risk management elements over which the EBMO is likely to have meaningful influence, and then feeding those elements back to the General Director and senior governance to ensure that the EBMO's stated strategic objective and mission is indeed consistent with its ability to deliver in the real world. This reporting structure would be effective in ensuring that ERM initiatives in the field are staying properly aligned with the strategic mission of the EBMO. As part of this mission, the ERM manager might also be charged with raising awareness of the issue of holistic risk management practices both within the member base and in society at large through active social dialogue. This is of value where a risk event might have an impact on the broader public, such as an oil spill or a cyber-attack on critical infrastructure. The message could be tailored to highlight to the positive actions taken by members with respect to risk management, while emphasizing the good the sector or the member organizations in general are providing to society.

In addition, the ERM manager might be responsible for designing process templates specifically tailored to the industry sector which it represents, facilitating the implementation of an ERM programme for smaller organizations that might feel they have neither the time nor the resources to commit to the process. For example, in the case of SMEs whose resources may be limited, the ERM manger or ERM department might be tasked with generating surveys and assisting in a process designed to

identify a comprehensive risk inventory for its members. The same could hold true for risk assessment, with EBMOs or the ERM manager providing customized sample risk scales for impact, likelihood, vulnerability, and speed of onset. They could encourage bow-tie analyses and provide scales for risk appetite to assist in developing appropriate risk responses.

The ERM manager could additionally customize sector-specific heat maps, risk dashboards and other communicative tools. Individual member organizations could use this as a starting point to ensure that any accelerating risk profiles are addressed immediately by their own appropriate personnel. In cases where an EBMO's own resources are limited it could nevertheless investigate and rank the myriad of third-party risk tools available online and seek to identify those vendors who might have capabilities specific to their industry sector. The ERM manager might also engage in many of the more traditional EBMO services, such as hosting networking events related to ERM to foster collaboration amongst industry leaders in areas of mutual interest. They might also be responsible for overseeing ERM consulting and advisory services, the offering of skills training and development programmes and more, but all with a specific focus towards best practices in a comprehensive enterprise-wide risk management programme.

Finally, the ERM manager or department could be tasked with aggregating risk management information across their industry sectors. As referenced, the resultant data can provide the basis for analytics, benchmarking, and the identification of surface trends, all of which might constitute invaluable information for individual members in terms of developing actionable responses related to the evolving risk landscape. Perhaps more importantly, in so doing EBMOs can provide summaries of best practices employed by its members to other members who may be further behind the curve, and to identify certain specific industry-wide risks inherent to their members' activities. They can also communicate and promote success stories in ERM which might exist within their membership base, resulting in even greater ERM adoption and membership uptake in what again becomes a virtuous circle.

Another practical way through which EBMOs might support members in this respect is by providing guidance for individual strategies related to specific risks. EBMOs, or the ERM Manager if applicable, can offer advice specific to individual members' particular vulnerabilities, both in helping to identify those vulnerabilities and in developing individual strategies to address them. EBMOs might have more impactful results by framing the issue as part of an overall strategy, effectively placing it in a larger context. Take for example a hypothetical manufacturing company who has identified potential vulnerabilities in its supply chain with respect to sourcing key components in the post-pandemic recovery (Figure 14).

▶Figure 14: Framing a specific risk in a larger context

Structure	ERM Programme Strategy (Example)	Verifiable Indicators (Example)
Goals	Ensure integrity of the supply chain in the face of pandemic recovery	Parts inventories at sufficient levels to run manufacturing process at 100% capacity
Activities	Actively search for alternative potential suppliers in different regions or countries	Submit Request for Proposal (RFPs); receipt of responses to RFPs a verifiable indicator of realistic options
Outputs	Develop lists of potential additional suppliers and their cost implications	In the event of supply chain disruption components sourced quickly from other suppliers
Outcome	Manufacturing processes continue to run at or near 100% with minimal disruption	Improved productivity and resilience

Source: Authors' elaboration.

Finally, the best laid plans are for naught without an effective implementation strategy. The message and the benefits associated with that message need to be clearly and succinctly communicated to members. Most members will have competing priorities and short attention spans when engaging with the EBMOs with whom they are affiliated, at least initially. In the digital age, the internet is the most likely means of projecting a message in a practical sense. The goal of course is to evolve to the point of personal interactions but to get there, an effective, succinct, and compelling online strategy is likely a prerequisite. This is as true with efforts directed towards ERM as with any other core message. From a practical perspective, two examples demonstrate how a value proposition might be effectively communicated online from the Norfolk Chamber of Commerce and the Canterbury Employers Chamber of Commerce respectively (Figure 15). An attention-grabbing headline, a clear and concise message which focuses on benefits in plain easy-to-understand language are some of the key components of effective messaging in the digital age.

▶Figure 15: Effective online communication – Sample value proposition

Source: Schmitt, Salvai and De Koster, 2021.

As noted, EBMOs have a strong advocacy role to play on behalf of their members, in shaping actual policy frameworks and the regulatory environment to place greater emphasis on the need to be prepared for what lies ahead. EBMOs can take this a step further. By utilizing sector-specific information collected from the membership base, EBMOs can be instrumental in developing industry and technical ERM standards to provide a baseline that members might eventually adopt and adhere to. This could well be an iterative process with governments, resulting in industry-wide standards leading either to guidance or regulation on risk reporting such as exists within the financial and insurance sectors. Many enterprises, particularly SMEs, are likely desirous of improving their resiliency in the face of emerging risks and black swan-type events but have little idea as to how to go about it. The provision of guidance or a regulatory framework could be just the roadmap a business requires. Moreover, as noted, the very act of collaborating with governments in the first place can serve to improve governmental relations with the potential for further positive impacts in additional lobbying or advocacy initiatives with respect to risk management.

EBMOs have a unique opportunity to partner with academic institutions, training centres, think tanks and NGOs, to further ERM research specific to their own industry sector's needs. An excellent example of academic leadership in the field of ERM is the NC State University's Poole College of Management Enterprise Risk Management Initiative, a programme dedicated towards cutting-edge ERM research, and more

importantly its application in the real world. Many universities have their own ERM programmes established within and specifically for their own institutions. Many other universities around the world offer degrees in risk management as part of their business administration and management programmes, and many of these are at the post-graduate or doctoral level. All these institutions could be potential partnership candidates that might work actively with EBMOs to promote state-of-the-art risk management. The question remains as to how to foster such relationships. It is likely incumbent upon a risk-focused EBMO to initiate first contact with academic institutions locally, and to explore whether such partnering opportunities might exist.

Partnerships with academia may take several forms. They may include for example private non-profit research, decentralized grant-funded research, and ad-hoc enterprise-academia partnerships. Such partnerships with academia can take on several structures such as those put forward by ILO (2020). These are the idea lab, the grand challenge, the extended workbench, and deep exploration. As an example of the idea lab, EBMOs can work with academics on short-term projects to explore new opportunities and alliances, potentially with a narrow focus towards a specific risk, or developing a sector-targeted risk management tool to address a particular issue. Within the construct of a grand challenge, EBMOs can partner with academics to work on longer-term ERM programmes and process development designed to create a new knowledge base that can be shared with both members and the public. While similar to the idea lab the extended workbench concept suggests that EBMOs can work with academia towards rapid solutions for individual risk assessment and sector-specific response to individual risks in some greater depth. Finally, within the context of a deep exploration, EBMOs can develop rich and enduring partnerships lasting years or even decades, ones that recognize ERM is itself an ongoing process, and that are able to respond to evolving ERM challenges and technologies as they might arise in the future. Both parties stand to benefit in this sort of deep collaboration, the academic partner in gaining greater awareness of real-world issues which might suggest additional avenues of research, and the EBMO in acquiring extensive core competencies which can be then disseminated amongst its constituents.

Finally, EBMOs can explore other partnerships and collaborations, involving various UN agencies for example, or those involving other key stakeholders across the value chain. EBMOs need to be flexible, adaptive, and forward thinking. They must be proactive in seeking out resources for ERM programmes that might exist but of which they are not presently aware, and in having done so then to actively communicate that knowledge to their members. This is the ideal real-world outcome. In practice however significant challenges exist, and even more so in the case of SMEs in the developing world

2.4. EBMOs can be drivers for ERM in SMEs

EBMOs, should they actively choose to do so, can be drivers of the development of ERM programmes in the case of SMEs. While this may sound good in theory, it is not so easy to put into practice. Significant challenges exist in implementing these concepts in any meaningful way, in both the developed world, and developing countries. In the global north for example, building productivity and resilience through ERM support initiatives requires a long-term strategic, and indeed one might say perpetual, commitment. It may take a significant amount of time before the outcome of such a strategy yields any quantifiable results, if indeed any at all. Risk events that have been identified, assessed, and planned for may or may not come to pass, resulting in a lack of measurable effects. Most of the largest enterprises have in-house risk management expertise upon which they can draw and are mindful of the positive impact of enterprise-level risk management. Many smaller organizations however are not likely to have in-house risk management expertise, thereby creating a knowledge gap between large multinationals and SMEs in general. Nevertheless, in the developed world at least, significant progress has been made, particularly with respect to education and managerial expertise. With an ever-increasing supply of risk management professionals on the market, modern risk practices are likely to disseminate from larger corporations to

smaller ones, eroding the traditional informational barriers that have plagued many smaller enterprises for much of the modern era. Another important challenge for EBMOs in this respect is encouraging the adoption of best practices in ERM amongst their membership bases. The issue of competing priorities and limited resources has been referenced, but it is true that many SMEs simply might not have come to recognize material, and potentially existential risks that threaten their organizational success. ERM-centric EBMOs have a good deal of work to do in raising awareness of the importance of comprehensive risk management programmes amongst its smaller constituents, as a necessary precondition of driving productivity and resilience, and enhancing enterprise value. Complexity also exists due to the many different groups of stakeholders involved, such as customers, investors, employees, suppliers, and various government actors. Many of these groups are likely to have competing agendas, or might at least perceive that they do, when in fact effective and holistic risk management programmes ultimately inure to the benefit of all concerned. Finally, as discussed, there are a multitude of commercially available tools and resources on the market, yet SMEs are the ones who are least likely to be aware of their existence, amplifying the need for EBMOs to raise additional awareness in this respect.

While challenges are evident in the global north, they exist to a far larger extent in the global south. Developing countries face a wide range of systemic and structural economic challenges. They tend to exhibit low rates of economic growth, low export levels, and low rates of foreign investment. Substantial portions of these populations, comprising close to a billion people in some 48 countries, face marginalization due to high levels of income inequality, and unequal access to social services, education, and health care (UN Global Compact, 2011). Other challenges include supply-side constraints, poor physical infrastructure, limited technical capacities, and an economic reliance upon a narrow range of commodities. Added to these burdens is often a weak and corrupt political system that threatens political stability. Poor people in developing countries tend to be hit the hardest by risks because the resources they have to manage risks are often limited or non-existent. As an example, more people die from drought in Africa than any other natural threat. In contrast virtually no one has died from drought in developed countries in many decades. Without improved risk management, the fight to create decent and resilient jobs in the developing world and ultimately to end poverty will be even more elusive. In such an environment, how then are EBMOs to further business resilience by nurturing a best-practices approach towards risk management?

The four tenets of decent work as articulated by the ILO are creating good jobs, guaranteeing respect for workers and the recognition of their rights, extending social protection, and promoting social dialogue (EBRD, 2021). Yet it is not enough to simply create good jobs in the first place, if these jobs are insufficiently resilient to withstand an increasingly volatile risk landscape. Good jobs need to allow for growth and long-term income security for workers. As discussed, levels of productivity and resilience amongst companies are influenced by many factors, one of which is undoubtedly the level of attention paid to risk management. There is little in the literature to suggest that EBMOs in developing countries are engaging with their constituents on the topic of risk management in any meaningful way, yet the opportunity to do so clearly exists. It is incumbent then upon the business associations themselves to take up the ERM mantle and promote it to their membership base. In so doing an EBMO stands to thrive with the renewed energy behind a revamped mission statement, while business resilience is enhanced across their industry sectors to the benefit of everyone involved.

Given the long-term perspective required in the adoption of an ERM programme, many SMEs in developing countries are likely to be somewhat daunted at the prospect. Many such enterprises transact their business on the very edge of viability in the first place, with little focus on long-term planning. When margins are razor thin, managerial focus tends to be on the micro-management of day-to-day crises. In this environment then, the issue of competing priorities becomes that much more acute. It is staggering that those organizations most at risk for disastrous outcomes are the least likely to

have modern risk management practices in place. Informational barriers and the knowledge gap are also much more severe. Developing countries are characterized by a lack of strong underlying institutionalized education in the first place, let alone in the training of the specialized skill sets required for state-of-the-art risk management. Weaker government institutions with respect to policy elaboration, regulation, and enforcement means that top-down government involvement is unlikely to provide the sort of risk compliance frameworks and roadmaps for companies to follow as often exist in wealthier nations.

These barriers in the global south represent significant obstacles in the adoption of any sort of ERM programme, and yet they do not stop there. The possible responses to a risk event were outlined in Chapter 1, including avoidance, transfer, mitigation, and acceptance, and in this respect SMEs in developing countries are severely limited. Avoidance simply may not be possible for SMEs as many operate at or near subsistence levels, with few options to avoid taking on the risk in the first place. It simply might not be possible to walk away from an inherently risky product or enterprise, as the activity might constitute the entirety of the business. The risks inherent in agriculture have been detailed herein, yet it is not possible for a subsistence farmer in sub-Saharan Africa to simply stop farming. SMEs in developing countries are also likely to have smaller networks of partners upon whom to draw for risk-based expertise. Not only does this serve to impair knowledge sharing and technological transfer, it can also significantly curtail responses based upon risk transference. Specific insurance products to deal with individual risks might not be available in the first place, or they may be too expensive to fit within what might already be a fragile business model. The concept of sharing risks outside of insurance, i.e., thorough joint ventures or co-ownership may also be severely limited, again due to the smaller networks in play and the fact that managers or owners of SMEs may simply have fewer opportunities to interact with people outside of the individual business itself. Mitigation options may also be minimal due to the scarcity of financial resources to implement them. At the end of the day this is likely to lead to what might be the riskiest response of them all, simply looking the other way and accepting risk as inevitable.

While obstacles exist for smaller enterprises, EBMOs themselves face their own set of challenges in developing countries. Many developing countries exhibit a dual structure in their domestic economies. On the one hand there are typically a few large, modern, well-capitalized and technologically savvy enterprises which wield a great degree of economic clout. At the other end of the spectrum there exists a majority of micro and small enterprises serving local markets with relatively simple and traditional management practices and technologies (Dyce, 2006). It is true that EBMOs can serve to provide its smaller members with the power of a collective voice. It is also true that the imbalance of economic power can be misused by an influential few for their own purposes, even within an EBMO setting, for example in areas of advocacy, or in shaping the strategic mission of the EBMO itself. Still, EBMOs serve an important function in improving the business environment of many developing countries, through collective advocacy, and by providing core services, skills training, and networking opportunities.

It is relatively simple to lump together developing countries as a homogenous unit when speaking in economic terms, however they are anything but. There can be significant cultural issues at work, depending upon the country, or region, in question. Cultural differences should not be underestimated. When people or enterprises of differing cultures adopt imported risk management practices and tools, they do so with internalized responses that have taken generations to embed. New tools and management techniques may be at odds with some of these responses, and a changing of the mindset can take time. Hillson (2018) points out that when importing risk tools and practices from the developed to the developing world, most companies are not deriving the benefits they expect. EBMOs can be instrumental in overcoming these hurdles, by promoting self-awareness of cultural influences that might affect how risk is perceived. EBMOs can help members focus on their own real needs, and not just upon what others might be doing. Simply copying others can lead to the adoption of systems that fail to add value to the enterprise; individual programmes, as always, need to be designed specifically for the individual enterprise. EBMOs can also assist in preparation, encouraging members to understand

the level of infrastructure required, and whether the necessary understanding, knowledge and skills are in place to implement an ERM programme. It is important that members be encouraged to adopt a measured, step-by-step approach. Implementation takes time, especially when tools and practices are being imported from a different culture. Trying to fast-track implementation of ERM can backfire, leaving the organization in doubt as to whether the adoption of a risk management programme was worth it in the first place. Finally, the risk approach needs to be tailored to the specific audience, to be compatible with the local culture and setting. Here too EBMOs can play an ambassadorial role in bridging cultural divides. It may be more effective in some circumstances to focus on personal interviews, while in other settings a predetermined survey may yield better results. Some cultures may not be inherently skilled in threat identification, others may fail to see opportunities. Risk management may be viewed as strategic in some cultures while merely a technical competency in others. Locally based EBMOs are well-equipped to navigate these complex cultural waters. EBMOs can be important intermediaries in this respect, by understanding the intricacies of the local culture on the one hand, and by championing the need for change when it can be proven to be in the best interests of its members on the other.

EBMOs in the developing country environment may also be faced with financial obstacles as well and may feel that they simply do not have the internal financial capacity to embrace a potential reset towards a focus on risk management. Their members may also face similar challenges, which can only serve to exacerbate the problem at the level of the business association. EBMOs are financed through a variety of mechanisms. Financing from members and third parties can include revenues generated from the constituent base, such as membership fees, contributions from members, local and international donations, sponsoring programmes whereby members can pay for enhanced visibility within the association, patronage by philanthropic foundations, crowdfunding and more. Additional funding is possible through subsidies or grants from a local public authority, although admittedly this practice is more prevalent amongst wealthier nations. A third means of funding is through financing from the activities of the business associations themselves. EBMOs may carry out commercial activities that generate a profit, provided that such profits remain within the association in furtherance of its social purpose. EBMOs can also organize fundraisers such as conferences, dinners, or shows. These types of events allow EBMOs to generate funds, while at the same time promoting and publicizing their activities, along with the added benefit of potentially attracting new members. Workshops, training events, seminars and consulting services can all generate additional revenues for the association. Many development agencies are increasingly supporting broader market and value-chain approaches towards development, by engaging with large and small companies alike, and with government authorities, donors, and other stakeholders to strengthen specific industry sectors

An EBMO operating in an a developing country would be well-advised to analyse the types of funding activities that are most pertinent within their own local contexts. An EBMO which decides to adopt risk management as a core and central focus might have new opportunities to revisit their traditional funding sources, or to adopt new ones with this fresh initiative at top of mind. Having defined a new strategic objective an EBMO might proactively approach the International Labour Organization (ILO) and global sustainable development financing organizations. The ILO can carry out an assessment of the business environment to address barriers to sustainable enterprise development and can provide guidance and technical assistance to develop an ERM programme.

International development banks, on the other hand, might be a source of funding for EBMOs worthy of pursuing. For instance, the European Bank for Reconstruction and Development (EBRD) has undertaken over 30,000 projects with SMEs across three continents. Part of the stated goal of the EBRD is to develop a local market for business advice, and consulting services that SMEs can take advantage of. In fact, the EBRD has launched some 28 separate SME support programmes throughout their countries of operations, including provisions for finance, business advice and policy reform interventions. Perhaps most importantly for purposes of this paper is that the EBRD also works in close

collaboration with all stakeholders, including EBMOs, trade associations and chambers of commerce, to improve the overall business climate for SMEs.

The World Bank publishes an annual World Development Report (WDR) with each year focusing on different themes, ranging from finance, global value chains, and the digital revolution to name a few. The WDR 2014, entitled Risk and Opportunity – Managing Risk for Development, stresses the need to move away from reactionary ad hoc responses to crises to more of a proactive, systematic, and integrated approach towards risk management. The report outlines a holistic approach to risk, very much in line with the ERM best practices set forth in Chapter 1. It suggests that appropriate risk management requires a collaborative approach involving shared action and responsibility at different levels of society, from the household to the international community. The report also recommends that individual countries set up national risk boards to assess and prioritize risks, and to coordinate public and private risk response actions (World Bank, 2013).

Opportunities exist for EBMOs to reach out proactively to the ILO and international development banks in their country to explore whether ERM-related partnerships might be possible within their own local context.

In summary, EBMOs have much to contribute to addressing these challenges, but it all needs to start with a clearly defined strategic vision. With that in place, EBMOs can educate members as to the inherent value for the business in adopting an ERM programme, and in doing so assuage concerns over the timeframes and costs vs benefits involved. Most organizations after all are in business to enhance their enterprise value over the long run. EBMOs can be instrumental in closing the knowledge gap, by providing educational and future oriented ERM skills training programs. They can be strong advocates for additional government funding to build resilience across their respective industry sectors, by highlighting the societal benefits of their members' activities and the need to protect them from the inevitable ravages of accelerating risks, such as the impact of climate change and geopolitical conflict that are already built into the system. They can assist members in navigating the complex array of ERM tools and programmes already in existence and produce new tools and templates for risk management specifically tailored to their individual industry sectors. They can aggregate and analyse risk and risk management data to provide benchmarking on risk management practices. They can engage in active social dialogue, to enhance corporate reputations and to highlight the corporate social responsibility and societal benefits delivered by their members through their activities, including a proactive approach to risk management. Finally, EBMOs can serve as a bridge to connect all stakeholders to promote a clear and resolute collective voice to promote coherent integrated risk policies to protect the interests of all those concerned.

References

ASHRM, 2022. ASHRM: Homepage | ASHRM. [online] ASHRM. Available at: <https://www.ashrm.org> [Accessed 14 June 2022].

Business Insurance, 2009. Risk Management Associations and Organizations - Business Insurance. [online] Business Insurance. Available at: <https://www.businessinsurance.com/article/20090526/story/218/risk-management-associations-and-organizations> [Accessed 14 June 2022].

CFA-FCA, 2022. Business Risk Management Programs | CFA-FCA. [online] Cfa-fca.ca. Available at: <https://www.cfa-fca.ca/issues/business-risk-management-programs/> [Accessed 15 June 2022].

Dohlman, E., 2020. USDA. [online] USDA. Available at: <https://www.ers.usda.gov/topics/farm-practices-management/risk-management/risk-in-agriculture/> [Accessed 15 June 2022].

Dyce, T., 2006. THE ROLE OF SMALL BUSINESS ASSOCIATIONS IN BUSINESS ENVIRONMENT REFORM. [online] Businessenvironment.org. Available at: <http://www.businessenvironment.org/dyn/be/docs/128/session4.4paper4.4.1dyce.pdf> [Accessed 18 June 2022].

EBRD, 2021. Donor support for small enterprises. [online] Ebrd.com. Available at: <https://www.ebrd.com/small-business-support/donor-support-for-small-enterprises.html> [Accessed 18 June 2022].

Friberg, A., 2022. About PURMA. [online] Purma.org. Available at: <https://www.purma.org/index.php?option=com_content&view=article&id=44&Itemid=27> [Accessed 14 June 2022].

International Labour Organization (ILO) (2020). Driving Up Productivity: A Guide for Employer and Business Membership Organizations. Global technical report, 04 November 2020. Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---act_emp/documents/publication/wcms_758749.pdf

Jain, S., Hagenbeek, O. and Shogren, B., 2021. Why global sustainability is important in business. [online] Simon-Kucher. Available at: <https://www.simon-kucher.com/en/blog/global-sustainability-study-what-role-do-consumers-play-sustainable-future> [Accessed 14 June 2022].

Mikhnev, A., 2006. building the Capacity of BMOs: Guiding Principles for Project Managers. [online] Ppd.cipe.org. Available at: <http://ppd.cipe.org/wp-content/uploads/2014/08/Building-the-Capacity-of-BMOs.pdf> [Accessed 5 April 2022].

NC State ERM Initiative, 2022. Executive Perspectives on Top Risks. [online] Erm.ncsu.edu. Available at: <https://erm.ncsu.edu/az/erm/i/chan/library/2022-executives-top-risks-report.pdf> [Accessed 14 June 2022].

PRMIA, 2022. Mission. [online] Prmia.org. Available at: <https://www.prmia.org/Public/About/Mission/Public/About/Mission.aspx?hkey=f2274f1c-a4e3-4751-817a-dde3b7364ed8> [Accessed 14 June 2022].

Schmitt, J., Salvai, P. and De Koster, A., 2021. MEMBERSHIP STRATEGIES AND POLICIES A manual for Employers and Business Member Organizations. [online] Itcilo.org. Available at: <https://www.itcilo.org/sites/default/files/2021-07/Membership%20Manual%20FINAL_web.pdf> [Accessed 27 May 2022].

UN Global Compact, 2011. Partners in Development How Donors Can Better Engage the Private Sector for Development in LDCs. [online] Standardsfacility.org. Available at: <https://www.standardsfacility.org/sites/default/files/UNGC_Bertelsmannn_web.pdf> [Accessed 18 June 2022].

World Bank, 2013. Managing risk for development: From crisis fighting to systematic risk management. [online] worldbank,org. Available at: <https://www.worldbank.org/en/news/feature/2013/10/06/Managing-risk-for-development-From-crisis-fighting-to-systematic-risk-management> [Accessed 18 June 2022].

▶ Conclusion

Risk is always with us. It exists for individuals, enterprises, governments, and society. Geopolitical conflicts, pestilence, famine, climate change, financial crises, they have all have been with us for millennia. Once thriving societies have faded away or been razed to rubble. In our evolutionary history, new forms of civilization have emerged from the ashes. Senior executives have widely reported their perception of the current risk environment as being increasingly precarious. People in positions of power and influence have likely thought the same throughout history, whether it was during invasion of the Greek city-states by the Persians, the lead-up to the fall of Rome to the Barbarians, or the two world wars, it might be argued that times are not necessarily more complex, rather that this is a natural state of being. What is perhaps more troublesome is that risk consequences are now more far-reaching than has ever been the case. Weapons of mass destruction and a century's worth of carbon pumped into the atmosphere have led many of us to realize that the very survival of our species is not necessarily a given. Perhaps this has something to do with why executives think the current environment is increasingly riskier, or perhaps it has always been thus. The purpose of this report is not to be pessimistic however, far from it.

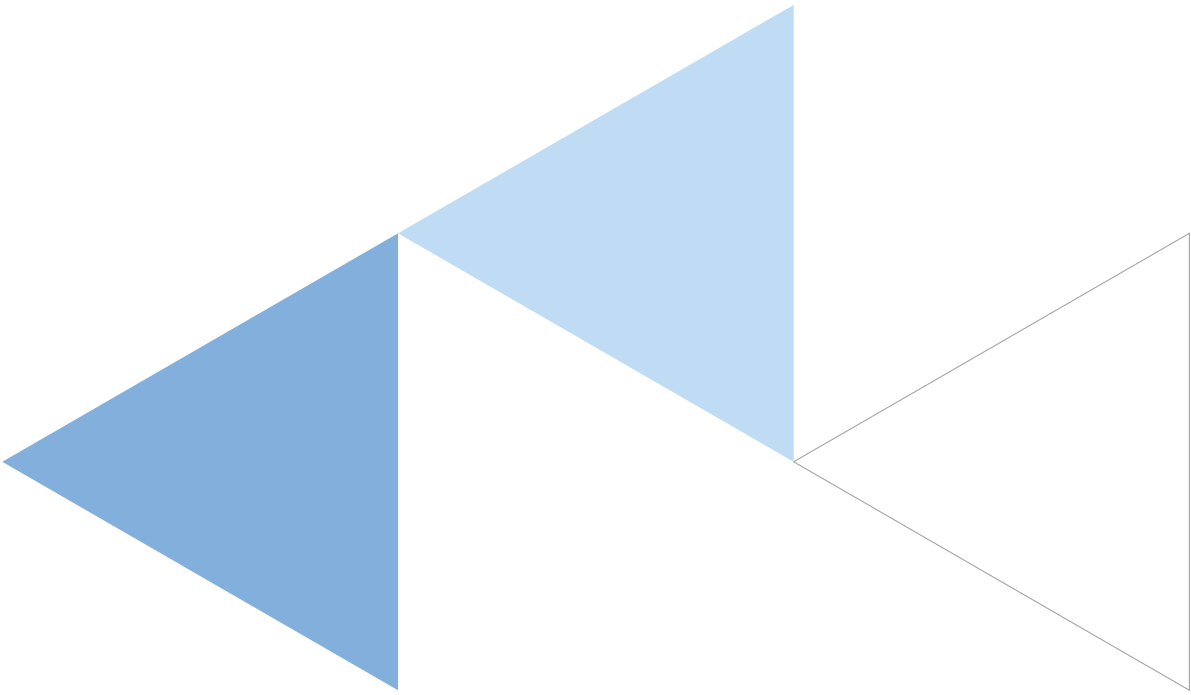
The fact that many business executives perceive an increasingly complex and dangerous risk environment, whether justified or not, is itself an opportunity. This mindset can inspire a greater openness towards considering the adoption of a holistic risk management approach for their enterprises. It is itself conducive to greater ERM adoption, and EBMOs can serve to be the catalyst that jump-starts meaningful change in this regard. The value proposition of EBMOs has been well defined herein, both in terms of their advocacy role and member services functions. To be effective in delivering value to its members, EBMOs must consider a long-term vision based upon adaptive planning and strategic foresight; this is true in all aspects of an EBMO's activities, and it is especially critical when dealing with the concept of risk.

For EBMOs without a particular emphasis on risk management, the opportunity to rebrand with a risk-centric focus provides the chance to re-energize the association. The benefits of the adoption of state-of-the-art risk management practices are clear. If increased productivity can be defined as increasing output with fewer and more efficient inputs, ERM provides a direct benefit. Unforeseen risk events undoubtedly have negative effects on output, both in terms of constraining an organization's ability to deliver goods and services, and in terms of diverting internal resources away from the enterprise's core strategic mission to deal with the crisis at hand. The case for bolstering resilience through ERM is self-explanatory. Business resilience is essential in providing long-term and decent employment, and in ensuring ongoing income security for workers. Risk events might not only be disruptive, but they might also be existential. This is especially true amongst SMEs in developing countries, many of whom may be operating on the very edge of viability in the first place. In finding ways to engage with such enterprises on risk management, EBMOs provide an essential benefit in enhancing the prospect of longevity amongst its individual members. At the same time, they are helping their own cause, by becoming more relevant to their constituents and enhancing their own reputations in terms of social responsibility.

Best practices in ERM have been discussed herein in some detail. There exist complexities in implementation of an enterprise-wide risk management programme, and when faced with a lack of resources or competing priorities there may be a tendency to not afford ERM the priority it deserves. This is especially true amongst SMEs in the developed and developing world alike. The problem is of course more acute in developing countries, where resources are thin and systemic structural inequalities are the order of the day. EBMOs must operate within their local context and on-the-ground realities, but they do have the tools, from assessing third-party ERM offerings, to hosting network events, aggregating,

and analysing sector-specific information, engaging members with skills training and more, to make a difference in risk management practices amongst their constituents should they so choose. Making the strategic choice is imperative. Very little is likely to be accomplished if an EBMO does not specifically reflect the importance of risk management in its core strategic values and mission statement.

EBMOs must be flexible and responsive enough to respond to a rapidly changing business environment and an evolving risks landscape, and to incorporate forward-looking ERM thinking into the development of future services for their members. In measuring EBMOs' success in influencing risk management best practices, communicating a coherent vision and having strong governance and organizational structures are at the core. Without clear communication of strategic goals and having in place strong foundation to back them up it is unlikely that a focus on ERM is to prove at all influential in this respect. One way of ensuring effectiveness is to appoint an ERM manager or create an in-house department or risk management committee. EBMOs should seek out partnerships with academia and development agencies that are active in their own local contexts. In developing countries, they must consider the local context when attempting to import western tools. All in all, EBMOs have a unique opportunity to promote coherent integrated risk policies by empowering a clear and resolute collective voice, and in so doing enhance business productivity, resilience, and overall enterprise value.



ILO Bureau for Employers' Activities (ACT/EMP)
▸ilo.org/actemp

International Labour Organization ILO
4 route des Morillons
CH-1211 Geneva 22 - Switzerland
▸ilo.org

ISBN: 978-92-2-038056-7