Journal of
Risk and Financial Management

MDPI

Communication

What's Wrong with Enterprise Risk Management?

John Fraser [1,†], Rob Quail [2] and Betty Simkins [3,*]

[1] Hydro One Networks Inc., Toronto, ON M5G 2P5, Canada
[2] Robert Quail Consulting, Toronto, ON M4E 3J5, Canada; quail.rob@gmail.com
[3] Department of Finance, Spears School of Business, Oklahoma State University, Stillwater, OK 74078, USA
* Correspondence: betty.simkins@okstate.edu; Tel.: +1-405-744-8625
† Deceased.

Abstract: Enterprise risk management (ERM) was introduced in the 1990s and has since become expected by boards of directors and regulators as a sign of good management and good corporate governance. However, many organizations struggle to implement ERM, and still seek practical advice on ERM implementation. This article explains many of the reasons why organizations are unsuccessful in their efforts at implementation and provides practical solutions provided by an experienced risk manager and consultant, an ex-Chief Risk Officer, and an academic, all of whom have written extensively on the subject. This article should be of interest to practitioners involved in implementing ERM, to consultants in ERM, and to academics teaching courses on ERM, risk management, and related topics. This article also provides a base against which further future research can be performed as ERM best practices continue to evolve.

Keywords: enterprise risk management; corporate governance; risk; risk management; COVID-19

Citation: Fraser, John, Rob Quail, and Betty Simkins. 2024. What's Wrong with Enterprise Risk Management? *Journal of Risk and Financial Management* 17: 274. https://doi.org/10.3390/jrfm17070274

Academic Editor: Thanasis Stengos

Received: 10 November 2023
Revised: 15 June 2024
Accepted: 19 June 2024
Published: 29 June 2024

1. Introduction

Over the last twenty years, enterprise risk management (ERM) has gained greater recognition as a key factor in good management and good corporate governance. Many regulatory bodies are now requiring boards of directors to be more involved in overseeing risk management, and most companies are seeking to implement ERM or key aspects thereof. For example, the Dodd–Frank Wall Street Reform and Consumer Protection Act recommended that foreign bank holding companies and U.S. bank holding companies (those over a certain size) establish a risk committee of the board, among other risk-related requirements.

Unfortunately, the success of ERM implementation has been less than expected. Beasley and Branson (2022) found that only 56% of large corporations reported having complete ERM processes in place. We have found that many organizations struggle with the implementation of ERM despite copious articles and the use of consultants.

In this *Journal of Risk and Financial Management* (*JRFM*) Communication article, we strive to fill an important gap in the literature. In the next section, we provide a brief background and review of the literature. In Section 3, we explain the reasons for these failures and provide practical advice on how to succeed. Based on our observations and experiences, we identify seven common problems with the way organizations go about implementing ERM. In the final section, we conclude, and describe future directions for ERM.

2. A Brief Background and Review of the ERM Literature

ERM can be viewed as the natural evolution of risk management. Kloman and Fraser (2021) put this development in context by providing a brief history of risk management, beginning in antiquity and leading up to 2019, including the description of several ERM milestones. In 1993, James Lam became the first ever 'Chief Risk Officer' (CRO) and is

widely recognized as a pioneer in the field of ERM. Because listed firms and organizations must employ an independent senior executive with responsibility for the risk management function (commonly referred to as the CRO), the CRO position has become common.

Many other articles and books have been written about ERM, including academic research, case studies, 'how-to' books/chapters, surveys, and white papers, among other formats. Regarding academic research, Pagach and Pascanik (2021) provide an excellent review of the literature and focus on four specific areas of ERM research: (1) academic studies investigating firms adopting ERM, (2) studies that identify firms' characteristics associated with ERM implementation, (3) research aimed at determining whether ERM creates value for organizations, and (4) academic business case studies on ERM. Refer to Exhibit 39.2 of their article for the 20 most-cited ERM academic journal articles.

Several case studies of leading organizations have been published referencing the successful implementation of ERM. For a book containing many ERM case studies on ERM best practices, refer to (Fraser et al. 2015). One of the earliest case studies is about the ERM early adopter, energy giant Hydro One, Inc. (Aabo et al. 2005; Mikes 2008; Fraser et al. 2021c). Hydro One has been at the forefront of ERM for many years, especially in utilizing a holistic approach to managing risks, and serves as a best-practice case study for other firms to follow.

Narvaez (2011) includes case-study examples to explain how various public organizations have adopted ERM. She provides examples from organizations such as the Department of Homeland Security, the Centers for Disease Control and Prevention, the Department of Education, the University of California, and Dallas Fort Worth International Airport.

Other examples of ERM best-practices case studies include the following:

- Mars, Inc. (Warner 2015): Mars is a global food company and one of the largest privately held corporations in the U.S. This case study describes how Mars recognized the importance of providing its managers with a tool to take risks knowledgably and comfortably in order to achieve its long-term goals.
- Statoil (Alviniussen and Jankensgård 2015): In this case study, the authors discuss ERM at Statoil, one of the top oil and gas companies in the world, now named Equinor. The case describes how, at Statoil, understanding and managing risk is considered a core value of the company, one which is written into the corporate directives and widely communicated to employees. ERM is thoroughly embedded in the organization's work processes, and its risk committee has managed the transition from a 'silo' mentality to the promotion of Statoil's best interests.
- University of California Health System (Crickette 2015): Crickette describes ERM at the University of California's (UC) Health System (composed of numerous clinical operations, including five medical centers). She describes how ERM plays an important role at the UC Health System and assists the organization in assessing and responding to all risks (operational, clinical, business, accreditation, and regulatory) that affect the achievement of the strategic and financial objectives of the organization.
- Bank of Tokyo-Mitsubishi (Nagumo 2005): Nagumo describes how the international banking giant Bank of Tokyo-Mitsubishi launched a global balanced scorecard as an enterprise-wide strategic management tool and integrated it with ERM.

There are many books providing advice on ERM. A few examples are described below:

- *Enterprise Risk Management: From Incentives to Controls*, 2nd Edition (Lam 2014): This book focuses on the 'what' of ERM. Lam describes both the art and science of effective ERM practices. This book covers key concepts, processes, and tools underlying risk management and highlights strategies to manage risk.
- *Implementing Enterprise Risk Management: From Methods to Applications* (Lam 2017): This book focuses on the 'how' of ERM implementation.
- *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, 2nd Edition (Fraser et al. 2021c): This book provides in-depth insights into what ERM managers are doing. This book also includes a chapter on teaching ERM,

and the pedagogical techniques described are being used at universities in the U.S. and Europe (see Lange and Simkins 2021).

Despite the wealth of published studies on the subject, many organizations still struggle with ERM implementation. Clearly ERM is not a one-size-fits-all exercise. Our article strives to fill this gap in the literature and hopefully will assist more organizations in achieving success in ERM implementation. In the next section, we describe common problems with ERM implementation and offer suggestions to overcome these challenges.

3. Common Problems with ERM Implementation

In this section, we describe in detail seven common problems that organizations encounter, impeding their ERM implementation. We provide guidance on how to avoid these pitfalls so that an organization can excel at ERM.

These common problems are the following:

1. An over-emphasis on reporting;
2. Not enough injection into the decision-making processes;
3. Too much adherence to a static process;
4. Treating risks as discrete items;
5. The misuse of models;
6. The belief that all risk is bad;
7. A lack of role-clarity.

3.1. An Over-Emphasis on Reporting

Here is a brief summary of what ERM was initially intended to accomplish. In 2000, before the International Organization for Standardization (ISO) and Committee of Sponsoring Organizations of the Treadway Commission (COSO 2017) standards were published, many early adopters of ERM sought to improve their competitive performance and increase value through rational, strategic, coordinated risk-taking; they sought to build transparent cultures where people were comfortable openly discussing risks and sharing their honest opinions about ways they might fail, i.e., to stimulate the conversations about uncertainty which are used to prioritize actions or alternatives or to allocate resources. From time to time, these conversations would result in artifacts such as reports or lists of risks and associated treatment strategies, which might be shared periodically with boards of directors and oversight groups to stimulate more conversations and build understanding of the role of uncertainty in the business. Reporting was a by-product of ERM, and not its central purpose.

Several things then happened which knocked many ERM practitioners off of this course in the early days. The first of these was the Sarbanes-Oxley Act (SOX) in 2002 (Sarbanes-Oxley Act 2002). At the time, many organizations 'lumped SOX in' with ERM. ERM conference agendas suddenly shifted from being about building more effective tools and processes to understand risk, to becoming focused on SOX implementation and reporting. In this way, ERM became seen as being more about assurance as to current controls, and about the present state of compliance, rather than uncertainties about the future.

The second disruptor was the widespread introduction of Governance, Risk, and Compliance (GRC) systems. This resulted in the emergence of increasingly intrusive and complex reporting tools, more and more elaborate reporting systems requiring many people to enter data into large databases for the purpose of tracking and reporting on compliance.

And then, third, there was a growing demand from boards for more and more risk reporting. On the one hand, that is a good thing: boards are becoming more sophisticated in terms of their understanding of their role in risk oversight (Fraser 2016). However, the problem is that, for many organizations, the central role of the ERM group has become the production of lists and reports on risks intended for consumption by the board, as opposed to actually helping the organization by enabling better decision making under uncertainty. One board director at a large, fast-growing company recently complained to one of the authors that the only time he ever saw risk assessments associated with major

proposals was post hoc, i.e., after the choice had been made. There were no conversations; it was purely one-way presentations to justify recommended courses of action. In his view, the organization was missing out on the benefits of discussing uncertainties associated with these major strategic choices with the board and receiving their guidance, advice, and perspective.

As a consequence of this massive shift toward ERM-as-reporting, in many organizations, managers' and executives' only interactions with their ERM groups consist of feeding periodic, quarterly, or annual bottom-up reporting cycles. ERM is not seen by them as a tool for making better decisions. Instead, it is seen as a way to describe or justify choices already made, or to placate senior management, boards, or oversight groups.

Recent experiences with COVID-19 are another good illustration of this. One of the authors is a member of the Strategic Risk Council (SRC) for the Conference Board of Canada, a round table of Chief Risk Officers (CROs) and other senior risk executives from a variety of sectors. When the COVID-19 pandemic first emerged, it seemed like an excellent research opportunity. Businesses were going through a once-in-a-century crisis, and all were going through it together, so it seemed like a good idea to diarise the collective experience of all these organizations' risk management groups. So, the SRC enlisted many CROs and had three or four different small-group video conference calls each week in which they shared what they were dealing with in real time. What they learned from those sessions was very disappointing, because many were working on similar, short-term problems such as how to have people working remotely, how to procure and distribute sufficient personal protective equipment, how to maintain supply chain integrity, and other immediate matters. Many CROs were engaged in assembling packages to placate their boards of directors and convince them that they were prudently managing the risks associated with the crisis. But few executives seemed to be asking the important risk-related questions, such as "What are the long-term implications for our business of this global event?" or "How might this event affect markets, or our competitive position with our customers or stakeholders?" Few seemed concerned with exploring the strategic implications of the pandemic. One organization actually shut down their entire ERM program for two years so the staff could help manage the current crisis.

The global pandemic presented a wonderful opportunity to demonstrate the value of ERM, and to help figure out these issues and understand the risks and opportunities. Surprisingly, most risk managers missed it. Why did they miss it? In many organizations, the ERM group is not seen as a support resource for making better decisions under uncertainty. Instead, they are seen as the 'heat-map people'.

Similarly, partway through the global pandemic, we published a paper providing recommendations as to how organizations should seize the opportunity during the COVID-19 crisis to consider the longer-term implications of risks to their operating environments (see Fraser et al. 2021a). This advice was largely ignored.

3.2. Not Enough Injection into Decision-Making Processes

In the 1980s, Nike wanted to 'own' the basketball shoes business. So, they went into big cities in the U.S. where kids were playing streetball. And they found the best players and gave them Nike shoes. They gave their shoes to the 'cool kids' so the other kids could see the 'cool kids' use the shoes as a tool to succeed, and so the other kids would want them, too (see, for example, Stonebrook 2021).

This is an excellent metaphor for the promotion of ERM within organizations. Find the people, either with the powerful processes or working on the messiest problems, who are open minded and willing to consider innovative approaches, and 'give them sneakers', i.e., give them tools, help support them in making better decisions and also in communicating the rationales for their decisions to their bosses. Almost without exception, in the authors' experience, every organization that has had ERM as a leading practice for a decade or more has followed that kind of approach: they identified the important processes or problems

in their business, and then found ways to customize their ERM approach so that it was a provocative force for improving those processes and helping to enable better decisions.

ERM must not be a silo. It must be a provocative agent, a disruptor. It is most effective when it gets injected into the most powerful, complicated, and risky decision-driven processes in the enterprise.

The following are several examples of specific ways to improve the impact of ERM through this kind of process-injection:

- Strategic planning. Risks are represented in the O (opportunities) and the T (threats) of SWOT. It is a natural fit.
- Business planning. Using bottom-up risk assessments as a driver for decision making and trade-offs about where to allocate resources, and ensuring the plans are aligned with the business strategy.
- Outsourcing. An outsourcing contract is not just the allocation of money and services; it also allocates risks between the two parties. So, why not transparently identify the risks related to the body of work that is being outsourced, use the contract to explicitly assign the risks between the two parties, and figure out how to make sure that they are oriented towards managing the critical things? (Quail 2021c).
- Investment prioritization. For every dollar available to the business, where should that money be used? One of the factors should pose the question of where that dollar can do the best in terms of mitigating risks and managing uncertainty about the achievement of the business objectives. Embed risk management right into those prioritization processes (Toneguzzo 2021).
- Technology projects. There is a saying that there is no better way for a Chief Information Officer to lose their job than to try and replace the enterprise resource platform or other enterprise technology in the business. It is risky work. Therefore, it follows that risk assessments should be done; not just according to the Project Management Office tools and methods, but in terms of scoping, resourcing, timing, vendor selection, and the all-critical go/no-go decision before 'go-live' and the resulting effects (Winters 2021).
- Regulatory compliance management. Many businesses are involved in very complicated regulatory environments, and it can be a challenge for organizations to prioritize areas for the allocation of resources for compliance management and control. Risk management can help organizations prioritize resources by exploring this question: Which of these regulatory requirements, if not met, has the bigger potential to cause harm or affect the achievement of the stated business objectives?

3.3. Too Much Adherence to a Static Process

The ISO 31000 risk management process is a good one (see ISO 2018). But one of the problems with any standardized process is that it implies that there is only one way to go about it. There are some great thinkers on the topic of ERM in academic circles, in particular Anette Mikes, Associate Professor of Accounting, Saïd Business School, University of Oxford, and Bob Kaplan, Senior Fellow and Marvin Bower Professor of Leadership Development, Emeritus at the Harvard Business School, who have written that they believe that the ISO and COSO standards came out too early, and that these standards have been a drag on innovation ever since. The models suggest that there is but one process that is the pathway to 'goodness' in terms of managing risks as a business (Kaplan and Mikes 2012).

But there are other useful, valid risk management processes; here are some examples:

- Black Swans, or extreme-end-of-tail risks (Taleb 2010). These risks are very unlikely but have the potential for extreme impact. The tools that one normally uses for prioritizing risks do not work anymore. Instead, one needs to identify other ways to learn from potential Black Swan-type scenarios as a kind of thought-experiment, i.e., if one of these scenarios occurs, is the organization resilient enough to be able to react in time, or at least faster and better than the competitors?

- Scenario planning exercises as pioneered by Royal Dutch Shell (see Schwartz 1991; Wilkinson and Kupers 2013). Remember, the ISO definition of risk is the effect of uncertainty on objectives. What scenario planning does is test to see whether those are the right objectives in the first place. In this way, it is about risks not to the strategy, but of the strategy. We note that, in the wake of COVID-19 and climate change concerns and the war in Ukraine, there has been a recent resurgence in the popularity of scenario planning.
- Custom criteria should be developed to help inform decision making, e.g., developing a technology road map for an organization by applying things like priority and opportunity in capacity, as well as an assessment of risks in the organization's ability to deliver.
- ERM can be dovetailed into strategy-setting through exercises like the risk appetite process (Quail 2021b; Ismail 2021).

In other words, there are ways to assess uncertainty and prioritize risks without going through the same old identify–assess–evaluate process as described by the ISO standard.

3.4. Treating Risks as Discrete Items

Most risk professionals who work in ERM generate lists of the top risks. Risks are brainstormed or extracted from a risk universe, or from a registry or some other source. They are assessed individually using some set of criteria and ranked. There may be some kind of roll-up for the organization or perhaps workshops or risk assessments with the executive team and senior levels of management. By whatever means, the risks assessed are ranked and delivered to the folks in charge to improve their understanding, and hopefully to stimulate conversations. For more information on risk management workshops, refer to (Quail 2021a).

However, risks do not act in isolation. Risks are not discrete elements. They are interconnected networks. ERM is a dynamic ecosystem. Failure of one part of the business can affect the success of others. For example, surprises in human resources might affect the performance in technology, and vice versa. Not enough work tries to understand and depict how risks interact or to fully map out the implications if a risk event actually occurs in one area.

Figure 1 provides a rudimentary example of a visual tool that can be applied to understand how risks are interconnected. In this fictitious organization that has outsourced its I.T. infrastructure management to control its risk and reduce cost, the risk of mismanagement of outsourcing can affect other things on the map. In the figure, the downstream impact of this outsourcing governance failure on other risks is depicted graphically. This is one simple example provided to illustrate what every risk manager should be doing—this kind of modeling, and the sharing of it with decision makers.

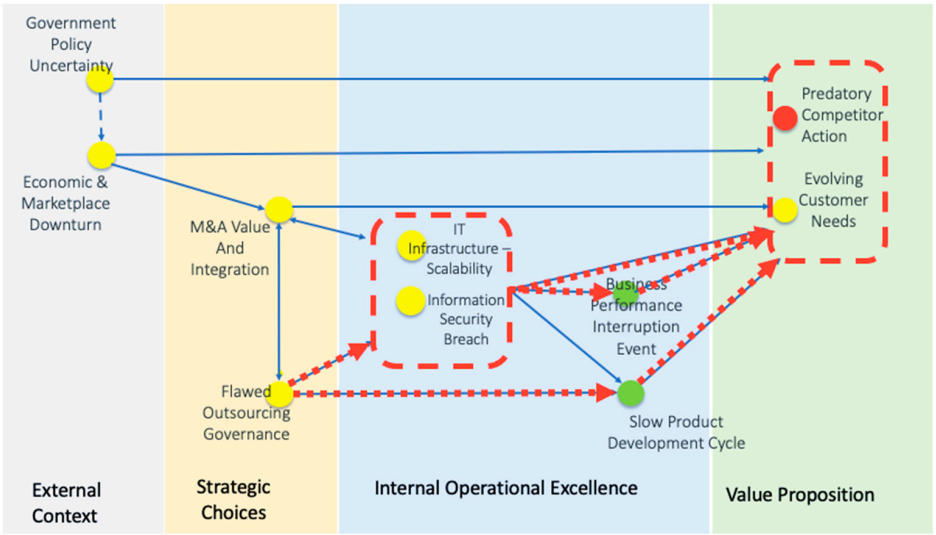

Figure 1. Graphical representation of risks' interconnectedness.

In the wake of the COVID crisis, which was immediately followed by the war in the Ukraine, businesses have been operating in a crisis mode or dealing with various fragilities or discontinuities in their business environment. Many aspects of their business, such as the supply chain or human capital, remain fragile. One should fully expect that any given organization will experience at least one major surprise—a 'second punch'—in the next few years. The question is the following one: can they take that punch, and do they know how risks could materialize, multiply, and/or accumulate? For additional information, see Winters (2021).

3.5. The Misuse of Models

Models are useful, but they are almost always wrong. In 1976, a British statistician named George Box wrote the famous line, "All models are wrong, some are useful." The real world is much more complicated a proposition than we can ever represent in a single model.

Figure 2 was posted on LinkedIn in 2021 by a 'risk expert' as a way to try to convince other people to use their services. What they said was that there are two potential investments, namely, Investment A at the top, and Investment B at the bottom, and there is a heat-map for each. Readers were supposed to choose one of the two investments based on the heat-map. The question itself was alarming in its naiveté. What was even more alarming, however, was the number of other 'experts' who tried to answer it.

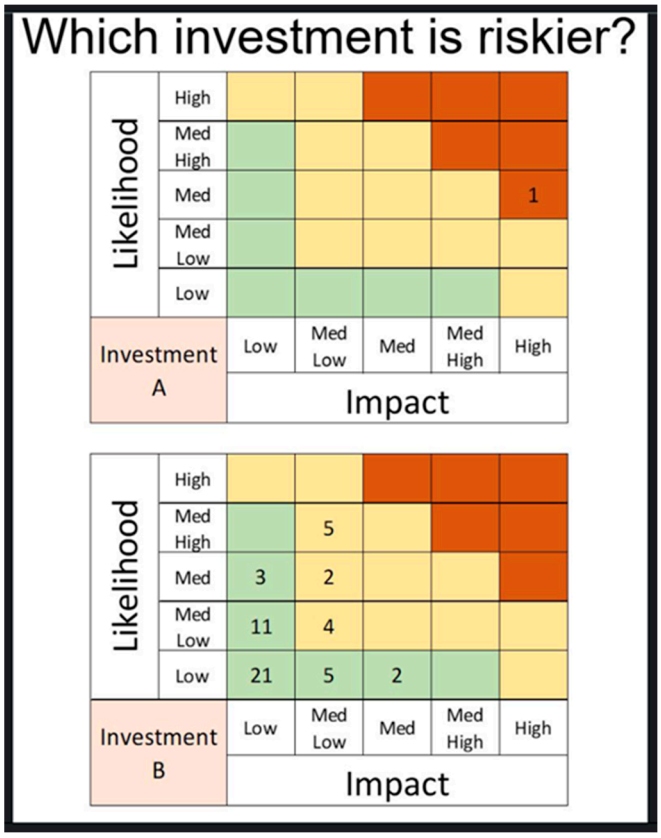

Figure 2. Misuse of models.

There are so many concerns with this question.

- First, a risk is not a single combination of impact and probability. A risk is associated with the range of outcomes of different probabilities; a risk is a curve, not a point. Now, usually when heat-maps plot risks, there is a spot on the map that represents something like a worst credible impact. But that is only for prioritization or to give a vivid summary picture for senior executives or the board of directors. It does not

convey nearly enough information to allow anybody to make any kind of actual decision.

- Second, the two risks in these two maps may not be defined in the same way. It could very well be the case that Investment B involves an array of lower level, more granularly defined risks, and that if you added them all up, they might add up to something that is at least as big as the risk in Investment A. So, that is another set of problems with heat-maps: the definition of the risk, the scope of the risk, and the scale used when evaluating the risks.
- In Investment B, should one of these risk events occur, there may be a domino effect, and once it finishes playing out, there may be a much bigger impact than was identified in the heat-map for Investment A.

Heat-maps have their very limited purposes, but this kind of decision making is definitely not one of them. And yet, dozens of risk 'experts' on LinkedIn thought that they could choose between these two alternatives based on these two heat-maps.

Models like heat-maps are only constructed to summarize priorities, encourage thinking, and stimulate conversations. They are not realistic depictions of decision-scenarios. Decision makers have to be reminded that risk models have limitations. Simple models like heat-maps are tremendous simplifications of very complicated realities.

The point is not just about heat-maps. In many cases, there can be real trouble because people trust the models too much. Speculative bubbles are consequences of people trusting valuation models too much. Various banking and financial crises have been about people putting too much faith in metrics, indices numbers, dollars and/or trends (Lowenstein 2000).

3.6. The Belief That All Risks Are Bad

Every organization (including hospitals, government agencies, churches, banks, and software companies), regardless of size, scope, or focus, is in the business of putting assets at risk with the expectation of it yielding some kind of return. It is how they make money; it is how they innovate; it is how they increase their influence; it is how they beat their competitors. They all put their assets at risk: their money or their intellectual property or their human capital or their reputation. Otherwise, nothing gets done. Risk is necessary. Risk is good.

However, many people, when they interact with ERM, seem to think that all risk is bad; there is a certain fixation on the downside.

There are two reasons why people perceive that risk is bad. First, it can be what they read, e.g., from regulators, and also from sources such as Sarbanes–Oxley and GRC. These are all about catching and reporting on non-compliance. Much of the upward reporting accomplished seems to focus on the bad things, the exceptions, and the gaps.

Second, it can be about where the ERM group reports organizationally:

- Some organizations combine risk and insurance. Insurance is about the avoidance of loss, i.e., the downside.
- Others have combined ERM with Internal Audit. The role of Internal Audits is basically to identify potential weaknesses in internal controls, i.e., the downside.
- Others place their ERM group in such a manner that they report to a General Counsel. What is the General Counsel's job? Avoiding legal or commercial risk exposures, i.e., the downside.

Consequently, there is the combined problem of using the wrong tools and reporting to the wrong places. This is why risk appetite is so important. Organizations need to understand their risk appetite and risk tolerance. What risks should be taken? What risks are deliberately chosen? There is no better way to enter into that kind of conversation than getting into an executive discussion about risk appetite. Quail (2021b) presents a practical method for developing a risk appetite that aligns with the strategic ambitions of an organization. One thinks about the different strategic objectives:

- For which ones do we expect that the pathway from where the organization is to where it wants to be is a squiggly/non-linear line, where the organization needs to be responsive and resilient? That suggests a higher risk appetite.
- Which of the strategic objectives are ones for which a small change or volatility in a key performance indicator (KPI) is going to indicate that the organization is lacking in control, and that it would be better to drop everything and figure out what is wrong? That suggests that there is a low risk appetite with respect to that objective.

3.7. A Lack of Role-Clarity

In the early years of ERM, many organizations started their ERM function as a spinoff from Internal Audit. The authors have noticed in recent years that there now seems to be a trend toward recombining these functions. More and more regulators are insisting that the Chief Risk Officer should be an independent assurance function that reports directly to the board of directors. Combining ERM and Internal Audit or assurance, or blurring their distinct roles in this way, can weaken both functions. Internal Audit is no longer independent. Also, ERM is no longer a 'safe' place to discuss risks and the adequacy of mitigation, because the person involved is also an auditor, and part of their job is to report to the board on weaknesses in internal controls and unmitigated risks. So, combining those two functions, or, in fact, combining ERM with any assurance function, is a problem.

There needs to be clarity in the organization as to exactly what ERM is to do. It is not just about producing reports for the board. It is not about providing assurance that the organization is in compliance with SOX. It is not about blowing the whistle when there is a risk about which the organization may think that it might be excessive. It is about helping to stimulate conversations in order to allow management to make better decisions about where the organization allocates resources, what risks to accept, and what risks won't be accepted. It is about building tools and models, all the while clearly communicating their limitations, to help support better decision making. For further reading on ERM and emerging roles in the implementation, refer to Mikes (2021) and Fraser et al. (2021b).

4. Conclusions and Future Directions

In this *JRFM* Communication article, we highlight past research and then present critical examples showing why many organizations fail or flounder in their attempts to implement ERM. Drawing on the extensive experience of an experienced risk manager and consultant, an ex-Chief Risk Officer, and an academic who has researched ERM extensively, we present both the causes and practical solutions in order to assist risk managers in being successful in their implementation of ERM. Numerous surveys show that the successful implementation of ERM trails the expectations of senior management, boards, and regulators (see, for example, Beasley and Branson 2022). This article provides specific practical explanations of the reasons for frequent failures, as well as simple, effective techniques and guidance on how to improve the chances of success in implementing ERM. We provide references for additional guidance on the ERM challenges presented.

ERM is still evolving, and new techniques and research are being explored on a regular basis. Organizations will continue to face business challenges, and risks will continue to evolve as the world becomes more complex. The world is now facing new and fast-evolving risks such as climate risk and the adverse effects of new technologies. There will continue to be unresolved risk issues. ERM will remain key in helping organizations adapt and change in order to remain resilient.

This article should be of interest to organizations implementing ERM, to academics teaching ERM, and to risk professionals desiring to learn more about this evolving process.

Author Contributions: Conceptualization, J.F., R.Q. and B.S.; methodology, J.F. and R.Q.; validation, J.F., R.Q. and B.S.; formal analysis, J.F. and R.Q.; investigation, J.F. and R.Q.; resources, J.F., R.Q. and B.S.; supervision, B.S.; writing—original draft preparation, J.F.; writing—review and editing, J.F., R.Q. and B.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: Author Rob Quail is employed by the company Robert Quail Consulting. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

Aabo, Tom, John R. S. Fraser, and Betty J. Simkins. 2005. The rise and transformation of the chief risk officer: A success story on enterprise risk management. *Journal of Applied Corporate Finance* 17: 18–31. [CrossRef]

Alviniussen, Alf, and Hakan Jankensgård. 2015. Chapter 24 Value and risk: Enterprise risk management at Statoil. In *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Edited by John Fraser, Betty J. Simkins and Kristina Narvaez. Hoboken: John Wiley and Sons, Inc.

Beasley, Mark, and Bruce Branson. 2022. *The State of Risk Oversight: An Overview of Enterprise Risk Practices*, 13rd ed. Raleigh: North Carolina State University Enterprise Risk Management Initiative.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). 2017. *Enterprise Risk Management—Integrated Framework*. COSO.

Crickette, Grace. 2015. Chapter 5 ERM in practice at the University of California Health System. In *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Edited by John Fraser, Betty J. Simkins and Kristina L. Navaez. Hoboken: John Wiley and Sons, Inc.

Fraser, John R. S. 2016. The role of the board in risk management oversight. In *Handbook of Corporate Governance*. Edited by Richard Leblanc. Hoboken: John Wiley & Sons.

Fraser, John R. S., Betty J. Simkins, and Kristina L. Narvaez, eds. 2015. *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Hoboken: John Wiley and Sons, Inc.

Fraser, John R. S., Rob Quail, and Betty J. Simkins. 2021a. COVID-19: The Risk Management Part Is Unfinished, CFO (January 21). Available online: https://www.cfo.com/corporate-finance/2021/01/covid-19-the-risk-management-part-is-unfinished-2699/ (accessed on 8 November 2023).

Fraser, John R. S., Rob Quail, and Betty J. Simkins. 2021b. The history of enterprise risk management at Hydro One Inc. *Journal of Risk and Financial Management* 14: 373. [CrossRef]

Fraser, John R. S., Rob Quail, and Betty J. Simkins, eds. 2021c. *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, 2nd ed. Hoboken: John Wiley and Sons, Inc.

International Standards Organization (ISO). 2018. *Risk Management—Guidelines*. ISO 31000. Geneva: International Standards Organization.

Ismail, Mohamed. 2021. Chapter 24 Organizational Decision Making. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, 2nd ed. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc., pp. 459–72.

Kaplan, Robert S., and Anette Mikes. 2012. Managing risks: A new framework. *Harvard Business Review* 90: 48–60.

Kloman, Felix, and John R. S. Fraser. 2021. Chapter 2 A brief history of risk management. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc., pp. 23–36.

Lam, James. 2014. *Enterprise Risk Management: From Incentives to Controls*, 2nd ed. Hoboken: John Wiley and Sons, Inc.

Lam, James. 2017. *Implementing Enterprise Risk Management: From Methods to Applications*. Hoboken: John Wiley and Sons, Inc.

Lange, David R., and Betty J. Simkins. 2021. Chapter 2 How to teach enterprise risk management: A Learner-centered activities approach. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.

Lowenstein, Roger. 2000. *When Genius Failed: The Rise and Fall of Long-Term Capital Management*. New York: Random House.

Mikes, Anette. 2008. *Enterprise Risk Management at Hydro One (A)*. Harvard Business School Case Study 109-001, July 2008 (Revised January 2012). Brighton: Harvard Business School Publishing. Available online: https://www.hbs.edu/faculty/Pages/item.aspx?num=36160 (accessed on 1 June 2022).

Mikes, Anette. 2021. Chapter 8 Becoming the lap bearer: The emerging roles of the chief risk officer. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.

Nagumo, Takehiko. 2005. *Aligning Enterprise Risk Management with Strategy through the BSC: The Bank of Tokyo-Mitsubishi Approach, Balanced Scorecard Report*. Reprint No. B0509D, September–October: 1–6. Brighton: Harvard Business School Publishing.

Narvaez, Kristina L. 2011. *Success Stories: Public Entities Adopt ERM Best Practices*. Alexandria: Public Entity Risk Institute.

Pagach, Donald, and Heather Pascanik. 2021. Chapter 39 A review of academic research on enterprise risk management. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.

Quail, Rob. 2021a. Chapter 19 How to plan and run a risk management workshop. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.

Quail, Rob. 2021b. Chapter 23 Risk appetite. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, 2nd ed. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc., pp. 459–72.

Quail, Rob. 2021c. Chapter 33. Risk management and outsourcing. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.

Sarbanes-Oxley Act. 2002. Senate and House of Representatives of the United States of America in Congress. Available online: https://www.congress.gov/bill/107th-congress/house-bill/3763#:~:text=Sarbanes-Oxley%20Act%20of%202002%20-%20Title%20I:%20Public%20Company,3)%20inspect,%20investigate,%20and (accessed on 8 November 2023).

Schwartz, Peter. 1991. *The Art of the Long View: Planning for the Future in an Uncertain World*. New York: Doubleday.

Stonebrook, Ian. 2021. How Sportswear Sold Streetball. *Boardroom*. August 12. Available online: https://boardroom.tv/sportswear-streetball-and1/ (accessed on 1 June 2022).

Taleb, Nassim. 2010. *The Black Swan: Second Edition: The Impact of the Highly Improbable*. New York: Random House.

Toneguzzo, Joseph P. 2021. How to allocate resources based on risk. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc., chap. 219.

Warner, Larry. 2015. Chapter 3 ERM at Mars, Incorporated: ERM for Strategy and Operations. In *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Edited by John Fraser, Betty J. Simkins and Kristina L. Navaez. Hoboken: John Wiley and Sons, Inc.

Wilkinson, Angela, and Roland Kupers. 2013. Living in the futures. *Harvard Business Review* 91: 118–27.

Winters, Mike. 2021. Chapter 36. Managing risk associated with project delivery: A how to guide. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Edited by John Fraser, Rob Quail and Betty J. Simkins. Hoboken: John Wiley and Sons, Inc.