Risk appetite: A crucial consideration for effective board risk oversight

Received (in revised form): 22nd January, 2024

Christopher E. Mandel

Instructor of the ERM Practice, Embry-Riddle Aeronautical University, USA

Christopher E. Mandel is full-time faculty at Embry-Riddle Aeronautical University where he teaches enterprise risk management (ERM) and is President of Excellence in Risk Management. His risk and insurance career spans over 40 years, where most of the time he was the senior-most leader of global risk management for several Fortune 500-sized entities, including his last role as chief risk officer for USAA Group. He was named Risk Manager of the Year in 2004 by the Risk Management Society (RIMS) where he served as president and seven-year board member. RIMS awarded him with its lifetime achievement award (Goodell) in 2016. He has numerous certifications and designations including Chartered Property Casualty Underwriter, Associate in Enterprise Risk Management, Risk and Insurance Management Society Certified Risk Management Professional and Associate in Claims, and he holds an MBA in finance from George Mason University. He is an influential, long-term thought leader in risk management and ERM.

1 Aerospace Blvd, Daytona Beach, FL 32114, USA
Tel: +1 210 845 5804; E-mail: MandelC@ERAU.edu or ExcelinRisk@gmail.com
LinkedIn Profile: https://www.linkedin.com/in/cemrisq/

Soubhagya Parija

Former Chief Risk Officer, FirstEnergy Corp, USA

Soubhagya Parija is the former chief risk officer at FirstEnergy Corp., a Fortune 500 power utility, and prior to that, for New York Power. He served on the board of RIMS and has had leadership positions both in retail and utility industries. He has had a long career defined by innovation, leadership and a commitment to enhancing risk management practices. He earned an MA in economics from Jawaharlal Nehru University, India, and an MBA in finance from Indiana University. He has also completed the Harvard Business Analytics Program.

76 South Main Street, Akron, OH 44308, USA
Tel: +1 914 393 4480; E-mail: soupar@gmail.com
LinkedIn Profile: https://www.linkedin.com/in/soubhagya-parija-9029224/

Abstract Progressive risk management has, among other things, inferred that effectively managing risk requires significant commitment to a risk appetite framework (RAF) that educates, trains and enables decision makers to make risk decisions in the context of understanding risk-taking capacity, preference and, ultimately, need. The starting point for this assumes a reliable measure of the current levels of risk has already been taken to understand the wherewithal to take incremental risk — taken for its potential to increase value. Yet, the need for commitment and investment by leadership can be hard to secure. Proving the value and reliability of a RAF is also not easily accomplished. Thus, RAFs have not been widely established across different industries, not nearly as much as in the financial services.

Research shows that proving RAFs' impacts on performance is necessary for successful implementation. Both the literature and testimonies of successful practitioners demonstrate that risk culture, strategic priorities, board risk oversight requirements, effective communications to stakeholders, reliable quantification of risk and a commitment to quality decision making that sufficiently considers relevant risks are all crucial to successfully managing risk taking guided by a RAF. Thus, after being properly designed, thoroughly tested and ultimately approved by senior management and the board, a risk appetite strategy (RAS) and RAF can be instrumental in more effectively managing and creating value, ultimately leading to a more resilient enterprise.

This paper will delve into the many elements of RAFs, allowing the reader to fully understand why management and governance should support their use. It will cover the challenges that practitioners face and how to resolve them. It will also provide a step-by-step methodology for designing, implementing and operationalising a RAS, including the roles of key players in doing so.

Keywords: *risk, risk appetite, risk oversight, risk tolerance, governance, performance, decision making*

INTRODUCTION

The concept of risk appetite has evolved significantly from traditional risk management, which primarily focused on mitigating downside, hazard-based risks. In today's dynamic and complex business environment, organisations are increasingly recognising the need to adopt a more proactive approach to all risks. They must embrace calculated risks to achieve sustainable growth and navigate uncertainty. To support this approach, several prominent professional bodies and organisations have incorporated the concept of risk appetite into their frameworks, standards and guidelines.

One of the most notable organisations to endorse and integrate risk appetite is the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO, a prominent audit and accounting-driven organisation, developed an enterprise risk management (ERM) approach that underscores the importance of risk appetite in its framework. COSO defines risk appetite as 'the amount of risk, on a broad level, an entity is willing to accept in pursuit of value'.[1] This definition encapsulates the essence of risk appetite and its relationship to value creation and preservation.

The International Organization for Standardization (ISO), a renowned, international standard-setting body, also recognises the significance of risk appetite. ISO provides guidelines for risk management in ISO 31000, emphasising the importance of establishing and communicating risk appetite and tolerances throughout the organisation.[2]

Additionally, the Institute of Risk Management (IRM),[3] a professional body dedicated to risk management research and best practices, acknowledges the crucial role of risk appetite in its guidance and resources for risk professionals. The IRM stresses the importance of defining risk appetite to align risk-taking decisions with organisational objectives; this is the risk–performance nexus.

In the UK, the Financial Reporting Council (FRC)[4] has also embraced the concept of risk appetite in its guidance and frameworks. The FRC, responsible for promoting high-quality corporate governance and reporting in the UK, recognises that risk appetite is a fundamental aspect of effective risk management. It helps organisations determine the level of risk they are willing to accept in pursuit of their strategic objectives and guides decision making regarding related risk-taking activities.

These endorsements from prominent professional bodies highlight the growing consensus on the importance of risk appetite in contemporary risk management. By incorporating the concept of risk appetite into their approaches, these organisations aim to enhance risk governance and board risk oversight, strengthen internal controls and promote transparency and accountability in financial and business reporting. The guidance provided by these bodies emphasises the need for organisations to define and communicate their risk appetite, assess and manage risks within their stated appetite and monitor and report on risk-related matters. Ultimately, the responsibility for overseeing risk appetite lies with the board of directors, which underscores its crucial role in the governance of risk. Figure 1 depicts this iterative hierarchy of the key components of a risk appetite framework (RAF).

While these guidelines emphasise the significance of risk appetite, it is interesting to note that, despite the widespread recognition of its importance, there are a limited number of examples of companies outside of the financial services industry that have successfully developed, implemented and operationalised RAFs. This apparent gap between

Figure 1: The key components of risk appetite

recognition and implementation can be attributed to several factors, including a lack of genuine understanding of the value proposition and the practical application of RAFs among boards and senior management. Nevertheless, there is plenty of evidence that the financial services industry has adopted and matured their approach to risk appetite strategy (RAS) and management as reflected in a 2020 survey of 50 banks by the International Association of Credit Portfolio Managers.[5]

One of the primary objectives of this paper is to address this gap by establishing why an effective RAF is crucial to effective board risk oversight. The concept of risk appetite will be explored in greater detail, providing clarity on its definition, components and practical applications. Additionally, the paper will delve into the distinctions between risk appetite, tolerances, limits and thresholds, offering insights into how organisations can navigate this complex landscape.

RAF COMPONENTS

Risk appetite is a fundamental concept in modern risk management that represents the total amount of risk that an organisation is willing to accept in pursuit of value, according to COSO.[6] However, understanding and defining risk appetite can be an elusive endeavour, as it requires a nuanced approach that considers numerous dimensions of risk measurement.

To grasp the essence of risk appetite, it is essential to distinguish between individual and organisational perspectives. Individual decision makers within an organisation, including executives and managers, will have their own risk preferences when it comes to risk taking. These individual appetites for risk may not necessarily align with the organisation's overall risk appetite, which is often not well defined. This diversity of perspectives about risk appetite is one crucial challenge to reaching a consensus on organisational risk appetite.

Organisational risk appetite, on the other hand, represents the collective view of decision makers within the organisation regarding the acceptable level of risk the organisation is willing to undertake in the aggregate. This collective perspective considers the organisation's overall risk-taking capacity, which is the maximum amount of risk the organisation can assume, at any given point in time.

The concept of risk appetite management assumes that an organisation has a fixed risk-taking capacity at any point in time and that it is crucial to ensure that cumulative risk-taking does not exceed this capacity. While most organisations have some idea of the risks they need to take to achieve their goals and objectives, explicit communication about, and alignment of, risk appetite are often lacking. This communication gap can pose challenges to effective governance, as decision makers may inadvertently exceed the organisation's risk-taking capacity without any awareness. Without a rigorous process for identifying those deviations, consistently effective risk management cannot be achieved.

One crucial aspect of risk appetite is its relationship with risk tolerance. Risk tolerance represents the acceptable level of deviation or variation from the organisation's exposures that decision makers are willing to accept. It is typically defined through key risk indicators and is applied at a more granular level, considering specific risk types, projects, business units or other segments. To illustrate this concept, consider a financial institution that has a risk appetite for credit risk. The organisation may establish a risk tolerance level for credit risk, expressed in terms of a specific threshold for various types of credit losses. If the actual credit losses exceed these thresholds, it triggers a need for further mitigation measures to bring the risk back

within acceptable bounds. Absent such action, an escalation protocol is necessary.

Beyond risk tolerances, organisations also use risk limits and thresholds to manage risk effectively. Risk limits represent the maximum level of risk that can be accepted before additional mitigation actions are required. In contrast, risk thresholds serve as early warning indicators, signaling that risk levels are approaching limits and prompting proactive risk management responses.

Understanding and effectively utilising these risk management concepts are essential for organisations seeking to optimise their decision-making processes while staying within acceptable risk boundaries. Failure to do so means the risk of failure rises. However, it is crucial to note that the terminologies and their related definitions associated with risk appetite, tolerance, limits and thresholds can vary among organisations. Inconsistent definitions and interpretations of these terms can lead to confusion and hinder the successful implementation of risk appetite strategies.

A CONSENSUS AMONG TERMS

The world of risk management is fraught with complex terminologies, and the nomenclature used in risk appetite management can quickly become a barrier to successful implementation. Business executives, including risk leaders themselves, may provide inconsistent definitions of core terms, exacerbating the potential for misunderstandings and misalignment.

To address this challenge, organisations embarking on the development of a RAF should prioritise the establishment of clear and consistent definitions for key terms. While it may not be necessary for all organisations to use all four terms noted above, it is essential to drive agreement on the interpretation of specific terminology to be used within the organisation's RAF.

Establishing clear definitions for these terms is foundational to effective risk management and governance. It enables decision makers at all levels of the organisation to communicate clearly and align their understanding of risk boundaries. Without consistent terminology, the execution of risk management processes can falter, beginning at the operational level and eventually impacting strategic decision making. Clarity in terminology ensures that both vertical and horizontal communication within the organisation is unambiguous, facilitating effective risk management execution.

While the use of all terms noted above is not essential to success, the following two terms are the heart of a RAF and RAS. 'Risk capacity' represents the total amount of risk that an organisation can assume, often determined by its financial capacity and balance sheet strength. It provides a quantitative measure of the organisation's ability to absorb risk without jeopardising its financial stability and long-term strategy. 'Risk target' represents the specific level of risk that an organisation needs to take to achieve its strategic objectives. It is a strategic consideration that guides decision making related to risk-taking activities in alignment with organisational goals.

Incorporating these additional terms into the organisation's risk management lexicon enhances clarity and precision in both discussions and actions about risk. It equips decision makers with a more comprehensive understanding of the factors that influence risk management strategies and actions. With a well-defined set of terms, organisations are better equipped to navigate the complexities of risk management and align their RAFs with their broader goals and objectives.

RAS

Now that a solid foundation for understanding risk appetite and its associated terminology has been established, it is time to delve into the details around the RAS, the key factor of a RAF. A RAS serves as the guide to an organisation's approach to managing risk in alignment with its objectives. It is, essentially, the compass that points decision makers in the right direction when it comes to navigating the risk landscape, in pursuit of a well-managed risk profile.

The following is a perspective on the RAS from an anonymous member of the Society of Actuaries:

> The conceptualized, practical, hands-on model of the enterprise risk objectives leading to assessment and implementation of the risk appetite and ERM program across the breadth and depth of

> an organization, with respect to business strategy and operations, to meet the stakeholders' goals and customers' satisfaction.[7]

COSO provides a perspective on risk appetite and the framework that reveals the connection to ERM, as follows:

> Appetite is only one part of enterprise risk management — one that does not operate in isolation. As set out in the Framework, appetite flows through all aspects of enterprise risk management. It needs to integrate with other parts of the business, from strategy development to implementation and monitoring.[8]

A RAF is a codification of an agency's strategic philosophy regarding risk. The term 'strategic' implies a specific, long-term view that leadership has taken regarding how organisational performance and objectives will be managed in relation to specific exposures deemed acceptable to stakeholders. The strategy is the starting point for the RAF, which enables decision makers to act consistently and transparently in matters related to risks that could otherwise prevent mission accomplishment.

THE RAF AND ORGANISATIONAL DECISION MAKING

Every decision comes with one or more elements of risk. Organisational decision making essentially involves manoeuvring around a series of trade-offs (ie risk versus rewards, long term versus short term, private versus public perspective, shareholders versus other stakeholders, etc). There is also a challenge in making decisions faster but with less information. Risk management data can be a great enabler of robust decision making. In today's rapidly changing business landscape, organisations face numerous uncertainties and risks. Having a well-defined RAF helps organisations navigate uncertainties with confidence and clarity. It helps answer the question of whether the organisation can accept the risk associated with a decision, and it helps answer the question of whether the decision made is optimal.

The following explores the key elements that affect how a RAF can significantly enhance organisational decision making.[9]

Balancing risk and reward: A RAF enables organisations to strike the right balance between risk and reward. By clearly defining the acceptable level of risk, decision makers can evaluate potential opportunities and challenges more effectively. This allows organisations to make risk-informed decisions that align with their goals while ensuring that risk taking is intentional, disciplined and focused.

Aligning strategic objectives and organisational mission: When decision makers understand the organisation's risk appetite, they can align their choices with the broader purposes of strategic objectives. This alignment minimises decisions that deviate from the organisation's mission and vision, reducing the likelihood of unintended consequences and misaligned actions.

Facilitating innovation: Innovation usually involves taking risks. A well-structured RAF encourages a culture of innovation by setting boundaries for acceptable risk taking. It enables employees to explore new ideas and initiatives within defined parameters, fostering a culture that encourages creativity and experimentation while still being mindful of potential risks.

Enhancing risk awareness: With an explicitly stated risk appetite, and a well-designed RAF, the various levels of the organisation can be trained to build a culture of risk awareness. Decision makers at all levels are more likely to consider the potential risks associated with various options before making choices. This heightened risk awareness helps in proactively managing and mitigating risks, reducing the likelihood of costly surprises.

Building resilience: A RAF contributes to organisational resilience by preparing organisations to withstand unexpected challenges. Decision makers can evaluate the impact of various scenarios and make contingency plans, ensuring the organisation can adapt swiftly to changing circumstances.

Strengthening governance and compliance: A RAF reinforces strong governance and compliance practices. Decision makers can assess whether proposed actions comply with the organisation's risk appetite and regulatory risk boundaries. This ensures that the organisation operates within its risk boundaries, reducing the likelihood of non-compliance and potential legal or reputational

consequences. This informs the board of interest in the management's drive to deliver the mission.

Enhancing stakeholder confidence: Organisational decision making is a complex process that involves a variety of stakeholders, including management, employees, customers, regulators and shareholders. A clear RAF considers potentially conflicting stakeholder interests and therefore instills confidence in these stakeholders. It demonstrates that the organisation is proactive in managing risks and making strategic decisions thoughtfully. This can lead to increased trust and credibility, benefiting the organisation's reputation and long-term success.

Effective risk appetite strategies undergird the RAF and share several crucial characteristics, including the following.

Alignment with an organisational strategy: A RAS must be closely aligned with an organisation's strategic and financial strategies. Since the consequences of risk can significantly impact an organisation's ability to achieve its objectives and financial performance, this alignment is crucial. It ensures that the goals underlying the RAS underpin the broader strategic objectives of the organisation.

Collaboration and consensus: Developing a RAS requires collaboration among various stakeholders, including executives, board members and risk professionals. Achieving consensus on the strategy is crucial, as it sets the priorities for the organisation's risk management efforts. The strategy should reflect the collective view of decision makers regarding risk taking and should be ratified by the appropriate governing bodies.

Clarity and transparency: A well-crafted RAS should be clear and transparent, providing decision makers with a clear understanding of the organisation's philosophy on risk. It should articulate the importance of using risk information to influence better decisions and maximise desired outcomes. Clarity in the strategy enhances communication and ensures that all stakeholders can easily comprehend the organisation's risk management philosophy and approach.

Integration with RAS: Following the ratification of the RAF, organisations should develop and ratify a RAS. This statement serves to document the consensus reached about organisational risk philosophy and put it into terms that are actionable by the stakeholder community. While high-level in content construction, it nevertheless provides clear guidance on the desired risk-taking behaviours of both leadership and day-to-day decision makers at all levels of the organisation.

RISK APPETITE AND BOARD RISK OVERSIGHT

Reflected in the experiences of many boards is the harsh reality of management and organisational failures that obviated the effectiveness of their risk oversight as directors and played out in the form of major, and sometimes catastrophic, losses to financial performance, reputation and brand equity. The typical view is of management's failure to execute according to plan or management's ethical lapses that produced fraud, corruption or other impacts. Whether one looks at the documented cause of Enron's implosion and demise (taking with it Arthur Andersen) or the collapse of Lehman Brothers in the wake of the 2008 derivatives crisis, forensic investigation proved that both boards failed in their oversight, in part because they had no objective measure of the amount of risk being taken by management and thus no way of knowing whether that risk taking was within boundaries set — either formally or, more likely, informally — and had limited means of verification.[10] These examples define, in part, what board risk-oversight ineffectiveness looks like. It is highly unlikely that a board can effectively oversee management risk decisions and risk taking without some discipline and rigour around appetite, capacity and targets. Put more simply, how can a decision about major risk taking be made or validated without knowing the answers to these seemingly simple (but in practice, not so simple) five key questions:

1. How much risk is management currently taking (risk profile) in the aggregate?
2. How much risk is management capable (capacity) of taking in the aggregate?
3. How much risk does management prefer to take (appetite) in the aggregate?
4. How much risk does management need to take (target) to execute strategy?
5. How does management close the relevant gaps?

Many assessments of management and organisational performance find that little or no discipline exists that would inform reliable answers to these questions. For example, a recent article published by Corporate Compliance Insights shows that executive management and the board are typically not on the same page with respect to the entity's risk appetite. The author, Jim Deloach, shares: 'typically, this means there has been insufficient risk appetite dialogue between the Board and management to obtain a high-level view of how much risk the entity is willing to accept and the risks the entity should avoid'.[11] If this is true, and reliable measures of the five questions above are elusive, then by default, management is managing risk informally and without discipline and can expect that some risk-taking decisions will be made in error and impact desired performance outcomes.

CHARACTERISTICS OF A GOOD RISK APPETITE STATEMENT

A risk appetite statement is both the first step in the process of building the RAF and the overarching evidence of how management views risk and risk management. Effective risk appetite statements share several key characteristics which distinguish them as valuable tools for decision makers and risk management. These characteristics include:

Direct linkage to organisational objectives: A well-designed risk appetite statement directly links risk taking to the organisation's objectives. It leaves no ambiguity about how risk should be managed in the pursuit of strategic goals. Decision makers can easily ascertain the alignment between their choices and the organisation's mission and vision.

Clarity and communicability: Risk appetite statements should be crafted to be clear and easily communicable. They are designed to facilitate smooth communication, monitoring and adjustment as needed. The language used in the statement should be interpreted by a broad audience, ensuring that all stakeholders can grasp its meaning.

Resource allocation guidance: Effective risk appetite statements provide guidance on resource allocation. They assist decision makers in prioritising resource allocation based on the organisation's risk appetite. This guidance ensures that resources are allocated efficiently and effectively to achieve strategic objectives.

Stakeholder communication: Risk appetite statements communicate clearly to both internal and external stakeholders. They convey the organisation's commitment to managing risks within defined boundaries and demonstrate a proactive approach to risk governance. This clarity instills confidence in stakeholders, promoting trust and credibility.

Portfolio perspective: Recognising that risks are interconnected and that decisions may impact multiple aspects of the organisation, a good risk appetite statement acknowledges the portfolio of risks that can mitigate each other. It considers the interdependencies between risks and helps decision makers navigate the complexity of the correlations among and between the risks in the portfolio.

An example of a well-constructed risk appetite statement would be as follows:

> The Organisation operates within a low overall risk range. The Organisation's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting and operations objectives. This means that reducing to reasonably practicable levels, the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations, will take priority over other business objectives.

Risk appetite statements serve as a crucial bridge between the overarching RAS and the day-to-day decision-making processes within the organisation. They would ideally be dynamic and subject to periodic revision whenever risk philosophy materially shifts. They provide a practical framework for translating the high-level strategy into actionable guidance that informs risk-taking behaviours at all levels of the organisation.

IMPLEMENTING AND OPERATIONALISING A RAF

The development of a RAS and associated risk statements represents the initial phase of implementing a RAF. However, the effectiveness of the RAF depends on its successful integration

into the organisation's processes, culture and decision-making mechanisms.

Operationalising a RAF involves a multifaceted approach, including the following key steps:

Data and analytics: Effective risk management relies on high-quality data and analytics. Organisations should invest in robust data collection and reporting systems that enable the measurement and monitoring of risk in real time. Data-driven insights facilitate informed decision making in alignment with the risk appetite.

Risk identification and assessment: Organisations must identify and assess risks comprehensively. This involves conducting risk assessments, stress testing, scenario analysis and using other techniques to evaluate potential risks to the organisation. The results of these assessments should be aligned with the RAS and inform decision making.

Integration with strategic planning: The RAF should be tightly integrated with the organisation's strategic planning process. This ensures that risk considerations are embedded in the development of strategic objectives and initiatives. Decision makers can then align their actions with the RAS from the outset.

Governance and oversight: Effective governance and oversight are essential for maintaining the integrity of the RAF. Senior management must assume responsibility for regularly reviewing and updating the framework to reflect changing circumstances and risk profiles. The board should review and affirm their concurrence with the essentials of the RAF.

Risk culture: Cultivating a risk-aware culture is vital to the successful implementation of a RAF. Organisations should promote a culture that encourages open discussions about risk, accountability for risk management and the use of risk information in decision making. A finely tuned strategy for both is essential to achieving targeted performance outcomes.

Reporting and communication: Transparent communication is key to ensuring that all stakeholders understand the organisation's risk appetite as it relates to the risk profile. Regular reporting on risk-related matters, including adherence to risk tolerances and limits, fosters trust and accountability.

Risk mitigation and response: When risks approach or breach defined tolerances or limits, organisations must have clear mitigation and response strategies in place. These strategies should be actionable and designed to bring risk levels back within acceptable bounds and designated time frames.

Training and education: Decision makers at all levels of the organisation should receive training and education on the RAF. This empowers them to make informed decisions aligned with the organisation's risk appetite. A fine-tuned strategy with effective measurement is essential to its effective use.

Continuous monitoring and review: The risk landscape is dynamic, and organisations must continuously monitor and review their RAF to ensure its relevance and effectiveness. Regular reviews and adjustments are essential to adapting to changing circumstances and stakeholder expectations.

External engagement: Organisations should engage with external stakeholders, such as regulators, shareholders and industry peers, to communicate their risk appetite and risk management practices. External validation and feedback can enhance credibility and trust.

EVIDENCE OF IMPACT

With risk appetite statements and strategies laying the foundation for the RAF, the necessary questions are: 'what difference do they make?' and 'do they have any impact on effective board risk oversight?'. In the IRM's publication 'Risk Appetite Statements', there are five detailed examples of a company's risk appetite statement and 31 firms with risk disclosures extracted from their annual reports, which demonstrate variations in risk appetite. The report states: 'It is also clear that the concept of risk appetite is gaining influence in these companies and the development and implementation of risk appetite statements is becoming a highly valued management process that enhances business success'.[12] While the direct correlation to performance outcomes — influenced by numerous organisational issues — may be difficult to validate, the mere fact that successful companies are willing to invest in RAFs and strategies shows that they are part of the success equation in those organisations.

Another argument for the value proposition can be found in an IRM paper developed by Crowe Horwath Global Risk Consulting, which outlines a valuation model where shareholder value is

influenced by operational issues, investment issues, sales growth, operating margin, tax rate, working capital, competitive advantage, discount rate cost of debt and debt cashflow from operational risks. The underlying shareholder value model is based on the hypothesis that shareholder value is calculated as the cashflow from operations, discounted by the weighted average cost of capital, minus the value of debt. Their proposition is that risks to objectives, which are normally connected in most ERM programmes, need also to be linked to the underlying shareholder value drivers. They posit that testing risks against models such as these will enable organisations to have a much better understanding of which risks are important at a much earlier stage of development and can thus be better managed before impact, by knowing and understanding the risk factors; doing so effectively means applying a RAF to the analysis.[13]

CHALLENGES AND CONSIDERATIONS

While the benefits of a well-implemented RAF are significant, organisations often encounter several challenges during the development and operationalisation process. It is essential to address these challenges proactively to ensure its successful implementation. Some common challenges include:

Resistance to change: Implementing a RAF may encounter resistance from employees who are accustomed to existing decision-making processes. Overcoming resistance requires effective change management and clear communication about the benefits of the framework. It also requires a mandate from the top of the organisation and recurring reinforcement by senior management to embed new behaviours in the organisation.

Data quality and availability: The effectiveness of a RAF relies on the availability and quality of data. Organisations may face challenges in finding, collecting and maintaining the necessary data for risk assessment and monitoring. Engaging stakeholders in these efforts will improve the chance of getting what is needed from the organisation to execute the RAF effectively.

Complexity and resource requirements: Developing and operationalising a RAF can be resource-intensive and complex. Organisations must allocate the necessary resources and expertise to ensure its successful implementation. They must also determine the acceptable level of complexity allowed by the culture or change the culture to accept new levels.

Integration with existing processes: Integrating the framework with existing decision-making processes (such as strategic planning and budgeting) reinforces its use. Ensuring alignment and consistency across processes is crucial, so that risk appetite is understood, embedded and actionable in every area of the organisation.

Risk measurement and quantification: Quantifying risk in a way that aligns with the RAS can improve its acceptance by users. Organisations may need to develop sophisticated risk measurement models and methodologies while ensuring that they resonate appropriately with users. This will be driven in part by the organisation's requirement for quantification of risk.

Cultural shift: Transforming an organisation's culture to embrace a risk-aware mindset can take time. Leaders must champion the cultural shift and set an example for others to follow. Reinforcement from the top of the organisation is essential to success in integrating the RAF into the culture.

BOARD RISK OVERSIGHT FAILURE

Returning to the risk professional's favourite risk management villain, Enron. Twenty years after their failure, it is clear that Enron's demise was accelerated by a board asleep at the wheel, among other things, including: inadequate and poorly implemented internal controls (when risk values must be known to apply controls effectively); a failure to exercise sufficient vigilance (when risk oversight in essence reflects a clear understanding of risk values as they relate to risk-taking decisions); a failure to respond adequately when issues arose that required a prompt and serious response (when risk exceeded risk-taking capacity, but where profits blinded them to reality); oversight as window dressing; failing to call for a review of crucial matters by the audit and compliance committee; the failure to insist on a proper information flow (when getting the right risk data to the right people at the right time must be a central goal of risk management); and an inability to fully appreciate the significance of some of the risk information with which the board was provided

(when significance is meaningless without reliable risk measures and understanding of risk thresholds).[14]

Revisiting Lehman Brothers' collapse provides another stark example of the failure of board risk oversight, as a 2014 Yale University case study[15] found that the board of directors did not effectively oversee Lehman and left it bankrupt. After Lehman collapsed, many observers have pointed out that it should not have taken excessive debt, it should have diversified its product portfolio and that the board of directors should have monitored its strategy and risk management more carefully. Most of the root causes of Lehman's failures can be traced back to the dysfunction of the board of directors.[16]

Our overarching premise for board risk oversight and management risk effectiveness is as follows: if you fail to accomplish a goal or objective — whether at the individual, departmental, business unit or enterprise level — it is likely because the parties involved have failed to manage one or more risks effectively. Furthermore, in order to manage all risks effectively, it is necessary to understand, and be able to rely upon, the five key questions outlined previously (see p. 6). Lacking reliable information about any of the five creates either a risk performance deficit or, in the case of the board's risk oversight accountability, an inability to successfully verify management's execution of risk-taking decisions. In both cases, shareholders and other stakeholders will be left wanting or worse.

To avoid risk oversight failure, risk should be embedded in decision-making processes to bring about the desired change in the behaviours of risk stakeholders, especially risk and control owners. To be truly effective in enabling the desired level and type of risk-taking behaviours, the RAF must be integrated into decision-making processes, including strategic planning, budgeting and resource allocation, portfolio management and project and programme approval and oversight. Decisions on the company's strategy must be informed by a view of existing and expected levels of residual risk (risk after mitigation) and set in the context of risk appetite. Risk-based resource allocation, within the context of a RAS and RAF, will enable resources to be deployed to help maximise risk taking to achieve the desired development objectives and to help manage key risk exposures.[17] When executed with these considerations, the likelihood of failure of board risk oversight will be materially reduced.

A RAF DEVELOPMENT PATHWAY

A 2022 survey by PricewaterhouseCoopers (PwC) confirmed through 3,500 respondents that risk appetite is, now more than ever, a crucial tool and that firms increasingly do not fully understand their risk profiles. They also found that taking on too little risk and missing opportunities for growth in today's volatile markets is a growing challenge. Surveyed firms show that they are starting to realise how a risk appetite can be helpful for managing growth through uncertainty. Specifically, a well-articulated risk appetite statement can help management and the board know that everyone is on the same page when it comes to taking risks. It helps in determining how well risks are being managed and where more risk can be taken in pursuit of growth. It also becomes a playbook for how much risk can be taken to meet strategic and operational objectives.[18]

A fully embedded RAF can be challenging to both design and achieve. As the PwC survey/report reflects, some disparity in the way risk appetite is operationalised may not always assist decision making or enhance risk management. A key issue is how RAFs often start as purely qualitative and may be viewed as bureaucratic and conceptual rather than actionable. Yet to be useful, RAFs mut be embedded into the organisation so they can be used to guide decisions and set triggers for escalating risks. To these ends, PwC's interpretation of the survey results depicted a 'pathway' for RAF evolution where most surveyed firms used a qualitative approach with many fewer respondents using a quantitative or embedded blend of both.[19]

When fully embedded, the RAF enables board risk oversight, providing reliable, actionable data for the board to assess the risk profile of the organisation and make clear judgments about the levels and extent of risk taking by any number of organisational segments. However, achieving reliable quantification of risks is the essential prerequisite to the operationalisation of the RAF. Reliable quantification requires investment in tools, techniques, processes and talent to bring it to life. The perceived return on this investment is often the

decision motivator that will either enable or frustrate deployment. To hurdle this potential barrier to success, more research is needed to demonstrate the verifiable return that every effective leader prefers to see before approving such investments and making related commitments to new processes.

CONCLUSION

The adoption of a RAF is no longer a luxury but a necessity for organisations operating in today's complex and dynamic business environment. It provides decision makers, both management and board leaders, with clear and actionable guidance for navigating risks in alignment with organisational objectives. Inasmuch as management is held accountable by the board, the RAF becomes one crucial tool to measure management success by, and ensure alignment between, risk taking and various ways in which that activity is bounded. Without it, neither management nor boards can make the best decisions, the most significant of which are almost always impacted by risks. By defining risk appetite, developing a risk appetite statement and strategy and operationalising the framework, organisations can enhance the quality of their risk governance, improve decision making, enable boards to fulfill their risk oversight responsibility more effectively and ultimately improve the likelihood of achieving both short and long-term objectives over time.

The codification and endorsement of risk appetite concepts and strategies by leading professional bodies and organisations, such as COSO, ISO, the IRM and the FRC, underscores the universal recognition of the importance of RAFs and RASs in contemporary risk management and governance. It reflects a global shift towards proactive and strategic risk management practices that go beyond risk avoidance to embrace calculated risk taking, tied to the strategic plan and mission accomplishment.

To successfully implement a RAF, organisations must overcome challenges related to user resistance, change management, data quality, complexity, cultural transformation and many of the biases that affect human decision making. The commitment of leadership, collaboration among stakeholders and ongoing monitoring and review of these elements are essential steps along this journey.

As shared in a recent COSO paper, 'Every Organization Must Accept that Taking Risks to Innovate and Grow Is Inherent to Business',[20] organisations must take risks to succeed, but risk cannot go unchecked. Establishing a discipline around risk taking is an important element of corporate governance, strategic planning and decision making. Determining appetite through a performance lens requires deep discussions that affect management and boards and, to be effective, permeate an organisation's culture. In this way, appetite reflects the mission and vision and integrates with strategy and objectives, with the end goal of adding value. Thus, if goal achievement is crucial to mission accomplishment and effective risk management is essential to achieving objectives, then managing risk to appetite (and with strategic discipline) is necessary for delivering performance outcomes that define success.[21]

A well-designed and effectively operationalised RAF empowers organisations to strategically harness the power of risk taking, aligned with quality decision making (see the Appendix). It enables them to pursue their objectives with confidence, make informed decisions and adapt to ever-evolving risk landscapes. By embracing risk appetite as a crucial element of board risk oversight and risk governance, organisations can navigate uncertainty, achieve resilience and thrive in an increasingly volatile and competitive business environment, while enabling boards to execute their risk responsibilities in a consistent and meaningful way.

APPENDIX: FOUR CASE STUDIES[22]

In an Executive Risk Report from the Risk Management Society, there are four 'case studies' briefly documented to demonstrate how four significant firms, in four different industries, are applying a RAF and related tools and concepts in order to more effectively manage risk. Each of these cases is a distinct example of the reality that applying RAF concepts differs at each firm in which it is applied. Regardless, each case example also demonstrates that these RAF tools and techniques are considered valuable enough to invest in and that by inference, they have some meaningful impact on performance outcomes sought and mission delivery.

‘CASE 1

Defining Acceptable Boundaries in Health Care

One non-profit health care organization considers its risk position in terms of boundaries. The combination of risk tolerance and risk appetite represents the organization’s “risk position” and demonstrates the degree of established commitment the organization has towards achieving its goal or expected outcomes (Figure 6, page 9). For this organization, risk tolerance is understood as the degree the organization is comfortably willing to absorb as potential losses in the pursuit of its goals, objectives and expected outcomes. Conversely, risk appetite is the degree the organization is willing to securely invest to exceed such measures. As such, it is important for the organization to pre-establish boundaries and set limits. Risk tolerance and appetite limits are set and act as triggers. This allows the organization room to react and reset a course of action when outcomes fall too far below or ahead of expectations. By monitoring results against the limits, the organization can determine when it begins to trend too quickly towards maximum tolerances (before reaching a “black swan” killer) or maximum appetites (when the pursuit of the “golden goose” no longer makes sense given the investment required). These boundaries are preferably set in aggregate but have been set against individual objectives, as well.

CASE 2

Public Risk Appetite Statements Disclosed by a Financial Organization

Consider the risk appetite statements disclosed by a major U.K.-based financial organization in its annual report. For this organization, risk appetite is defined using a combination of qualitative and quantitative statements. “Risk appetite is the amount and type of risk that [the organization] regards as appropriate for it to accept in order to execute its strategy. The board regularly reviews and sets this in the form of 10 risk appetite statements, which it sets in the context of [the organization’s] strategy and the requirements of various stakeholders, including the regulatory framework in which we operate.” The risk appetite statements provide the benchmark against which the company’s risk profile is reported, monitored and managed by the board, audit and risk, finance, and risk assurance committees. Risk appetite also forms the basis for the calibration and setting of the delegated authorities and financial limits for all aspects of market, credit, liquidity and operational risk. The 10 risk appetite statements address both quantitative and qualitative aspects of risk taking. The quantitative risk appetite statements address: • maximum tolerance for market, credit and operational losses • the maintenance of a minimum credit rating level • minimum economic and regulatory capital surpluses • the maximum earnings volatility • minimum excess liquidity resources to meet peak stressed liquidity requirements without the need to liquidate assets or raise capital The qualitative risk appetite statements address: • regulatory risk • reputation risk • business mandate • operational risks in the execution of business plans • risk-related decision making, especially in relation to new business opportunities. The statements express the organization’s risk-taking approach for its internal and external stakeholders. The statements paint a “portfolio” view of the organization’s willingness to bear and pursue risk for an expected return. It represents a collection not only of the risk types related to the business portfolio (qualitative statements) but of its overall enterprise financial appetite (quantitative statements). What is not clear—looking only at the statements themselves—is how these risks relate to each other within the organization’s overall risk portfolio. The public statements of the company do not indicate whether this particular organization uses an efficient frontier model to consider the interrelatedness of its risk/return decisions in a portfolio view. However, it may be safe to assume that at least some portions of its risk portfolio are considered in this way.

CASE 3

Toy Manufacturer Makes Risk/Reward Trade-Offs in Daily Management

Consider a very successful and innovative toy manufacturing company. This example highlights two high-level organizational risk appetite statements that are then used for decision making, whether in general for the company or as applied in

particular for each project. Appetite Statement Part 1: The company will not accept any risks that will be a "High Risk" after mitigation. The company is willing to bear or retain risks that are assessed as medium or low after mitigation in pursuit of its objectives. In this way, risk appetite is tied to the traditional risk map and the variability around earning levels. It is adaptable in that—based on how risk is characterized within the organization's earnings at any particular time—it can reflect either a higher risk appetite (Figure 7, page 10) or a lower risk appetite (Figure 8, page 10) as described more fully below. In this example, three risk priorities levels (High, Medium and Low) were determined when creating the risk map. Figure 7 reflects a relatively greater willingness to accept risk in pursuit of the organization's mission and objectives. The actual risk appetite can be modified based on the company's determination of "High Risk." If circumstances change and it prefers to adopt a lower risk appetite, it can designate "High Risk" to encompass lower impact levels as shown in Figure 8. However, this does not change the risk appetite statement itself. Appetite Statement Part 2: The company shall ensure that it materializes at least [x%] of the budgeted earnings at a 95% confidence level. Suppose the company wants to be 95% certain that earnings exceed $160 million. If budgeted earnings are set at $200 million, management determines that the acceptable lower range limit (or boundary) is 20% of budgeted earnings, that is, $40 million. Therefore, if actual earnings are above $160 million in 19 out of 20 quarters, they will have met their objective. To arrive at this situation, the company looks at the assumptions used in calculating the budgeted earnings as well as its risk portfolio and determines through simulations that the worst-case scenario at the 95th percentile is an acceptable value of 20% below budget (i.e., all but 5% of the scenarios result in budgeted earnings of at least $160 million). This means that all things being equal, only once in 20 quarters will the actual earnings be less than $160 million. In this process, management has determined that up to a 20% "miss" on earnings is acceptable, i.e., within its risk tolerance range. The major benefit of defining the risk appetite in this way is that the board and senior management understand the methodology and calculations enough to trust it. There are certain occasions when senior management or the board asks whether the company is taking enough risk and what would happen if they accepted more risk? The solution would be to compare the utilized risk capacity with the available risk capacity. If the company is far from utilizing the full extent of it, solutions involving being more aggressive and taking more risks are considered. In any situation, the available risk capacity will not be exceeded and considering the risk appetite, will be better utilized. Using a driving analogy, the condition of your vehicle may determine that you can safely drive 50 mph (available capacity). If you are currently doing 35 mph (utilized capacity), you may decide to go faster, as long as you do not exceed 50 mph.

CASE 4

University System Calculates and Articulates Its Risk Appetite and Tolerance Levels

Consider the case of a major university system comprised of multiple campuses, medical centres, research operations, student activities and housing, international facilities and programmes, and all that it entails. Two key questions need to be answered: 1. How should the appetite for any particular risk be determined and what should be measured? 2. What metrics should be used to measure whether the risk is within expected tolerance levels? One risk appetite statement and one set of metrics obviously would not serve the multiple stakeholders represented by the university system's environment. If set too low, a single risk appetite statement may be constraining. If set too high, it would provide little or no guidance to a number of the system constituencies. Ideally, the statements would provide: • Measures that reveal when deviations from expected outcomes are reaching or breaching the risk tolerance limits for each type of risk. Awareness and monitoring of established thresholds would help this organization track changes in risks and avoid unexpected consequences. • Risk targets that are the ideal goal for the risk based on the organization's objectives, risk appetite statements and measures for each risk. • Risk tolerance/range where risk would be allowed to deviate around the defined risk target. This ensures that defined risk

tolerances fall within the organization's risk capacity. The university's board of regents and management may establish a fairly high-risk appetite, but the system may not have enough capacity to handle a risk's potential volatility or impact over the breadth of the university system's operations. In order to manage within this environment, a system-wide team has explored a number of complementary approaches: • Combine the systems already established key performance indicators with the appetite and tolerance levels. • Allow the campuses to set their own thresholds based on a system-wide tolerance statement. • Use the already established enterprise risk management information system dashboards for communicating levels and reporting deviations from the expected outcome.'

References

1 Martens, F. and Rittenberg, L. (May 2020) 'Risk Appetite Critical to Success, Using Risk Appetite to Thrive in Achieving World', COSO, p. 1, available at https://www.gerenciandoriscosemprojetos.com/wp-content/uploads/2021/06/COSO-Guidance-Risk-Appetite-Critical-to-Success_v3.pdf (accessed 2nd February, 2024).

2 International Organization of Standards (2018) 'Risk Management Guidelines', ISO31000, available at https://cdn.standards.iteh.ai/samples/65694/60673072317a4b96bd36efb910b68926/ISO-31000-2018.pdf (accessed 2nd February, 2024).

3 Anderson, R. (n.d.) 'The Institute of Risk Management, Risk Appetite and Tolerance Guidance Paper', The Institute of Risk Management, available at https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf (accessed 2nd February, 2024).

4 Beasley, M. and Martens, L. (16th June, 2020) 'Video Discussion on COSO Thought Paper on Risk Appetite', available at https://erm.ncsu.edu/library/article/cosos-thought-paper-on-risk-appetite (accessed 2nd February, 2024).

5 International Association of Credit Portfolio Managers (2020) 'Risk Appetite Frameworks — Frameworks Proving Sound Amid the Current Covid Credit Crisis (Survey Of 50 Banks)', available at http://iacpm.org/wp-content/uploads/2021/04/IACPM-RAF-White-Paper-2020.pdf (accessed 2nd February, 2024).

6 Shang, K. and Zhen, C. (March 2020) 'Risk Appetite: Linkage with Strategic Planning', CAS/CIA/SOA Joint Risk Management Section, available at https://www.soa.org/493898/globalassets/assets/files/research/projects/research-risk-app-link-report.pdf (accessed 2nd February, 2024).

7 Banerjee, D. (2013) 'The ERM Framework of Risk Appetite: Risk Appetite Assessment', Presented at the 2013 Enterprise Risk Management Symposium, April 22–24, p. 5, available at https://www.soa.org/globalassets/assets/files/resources/essays-monographs/2013-erm-symposium/mono-2013-as13-1-banerjee.pdf (accessed 2nd February, 2024).

8 Martens and Rittenberg, see ref 1 above, p.13.

9 Dixon, D. (4th January, 2017) 'Five Steps to Developing a Comprehensive Risk Appetite Framework', *Wall Street Journal*, available at https://deloitte.wsj.com/articles/five-steps-to-developing-a-comprehensive-risk-appetite-framework-1483592543?tesla=y&tesla=y (accessed 2nd February, 2024).

10 Peregrine, M. and Elson, C. (5th April, 2021) 'Twenty Years Later: The Lasting Lessons of Enron', Havard Law School Forum on Corporate Governance, available at https://corpgov.law.harvard.edu/2021/04/05/twenty-years-later-the-lasting-lessons-of-enron/ (accessed 2nd February, 2024).

11 DeLoach, J. (23rd January, 2014) '10 Ways Board Risk Oversight Can Fail', Corporate Compliance Insights, 12th January, 2014, p. 1, available at https://www.corporatecomplianceinsights.com/10-ways-board-risk-oversight-can-fail/ (accessed 2nd February, 2024).

12 The Institute of Risk Management (2017) 'Risk Appetite Statements: Risk Snapshot', p. 14, available at https://www.theirm.org/media/4666/0926-irm-risk-appetite-12-10-17-v2.pdf (accessed 2nd February, 2024).

13 Anderson, R. (n.d.) 'Risk Appetite and Guidance Paper', The Institute of Risk Management,

available at https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf (accessed 2nd February, 2024).
14 Lipton, M. and Lipton, W. (3rd January, 2024) 'Thoughts for Boards: Key Issues In Corporate Governance for 2024', Harvard Law School Forum on Corporate Governance, available at https://corpgov.law.harvard.edu/2024/01/03/thoughts-for-boards-key-issues-in-corporate-governance-for-2024/ (accessed 2nd February, 2024).
15 Wiggins, R., Piontek, T. and Metrick A. (2019) 'The Lehman Brothers Bankruptcy A: Overview', *Journal of Financial Crises*, Vol. 1, No. 1 (39–62), available at https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=1000&context=journal-of-financial-crises (accessed 2nd February, 2024).
16 Kim, Y. A. (28th April, 2016) 'The Agency Problem of Lehman Brothers' Board of Directors', *Illinois Business Law Journal*, available at https://publish.illinois.edu/illinoisblj/2016/04/28/the-agency-problem-of-lehman-brothers-board-of-directors/ (accessed 2nd February, 2024).
17 Cline, M. and McCaffrey, C. (18th January, 2021) 'Ten Lessons Learned In Implementing Risk Appetite Frameworks', EY Global, available at https://www.ey.com/en_gl/consulting/ten-lessons-learned-in-implementing-risk-appetite-frameworks (accessed 2nd February, 2024).
18 PwC (2023) 'The Importance of Understanding Your Risk Profile and Appetite', available at https://www.pwc.com.au/about-us/insights/non-executive-directors/the-importance-of-understanding-your-risk-profile-and-appetite.html (accessed 2nd February, 2024).
19 PwC (2023) 'From Threat to Opportunity: PwC's Global Risk Survey 2023', available at https://www.pwc.com.au/publications/global-risk-survey.html (accessed 2nd February, 2024).
20 Martens and Rittenberg, see ref 1 above, p. 11.
21 *Ibid*.
22 Crickette, G. *et al.* (2012) 'RIMS Executive Report: The Risk Perspective Exploring Risk Appetite and Risk Tolerance', RIMS, available at https://docplayer.net/7721377-Rims-executive-report-the-risk-perspective.html (accessed 2nd February, 2024).