1

An Introduction to Enterprise Risk Management

1.1 Definitions and Concepts of Risk

The word 'risk' has a number of meanings, and it is important to avoid ambiguity when risk is referred to. One concept of risk is uncertainty over the range of possible outcomes. However, in many cases, uncertainty is a rather crude measure of risk, and it is important to distinguish between upside and downside risks.

Risk can also mean the quantifiable probability associated with a particular outcome or range of outcomes; conversely, it can refer to the unquantifiable possibility of gains or losses associated with different future events, or even just the possibility of adverse outcomes.

Rather than the probability of a particular outcome, it can also refer to the likely severity of a loss, given that a loss occurs. When multiplied, the probability and the severity give the expected value of a loss.

A similar meaning of risk is exposure to loss, in effect the maximum loss that could be suffered. This could be regarded as the maximum possible severity, although the two are not necessarily equal. For example, in buildings insurance, the exposure is the cost of clearing the site of a destroyed house and building a replacement; however, the severity might be equivalent only to the cost of repairing the roof.

Risk can also refer to the problems and opportunities that arise as a result of an outcome not being as expected. In this case, it is the event itself rather than the likelihood of the event that is the subject of the discussion. Similarly, risk can refer to the negative impact of an adverse event.

Risks can also be divided into whether or not they depend on future uncertain events, on past events that have yet to be assessed or on past events that have already been assessed. There is even the risk that another risk has not yet been identified.

When dealing with risks it is important to consider the time horizon over which they occur, in terms of the period during which an organisation is exposed to a

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

particular risk, or the way in which a risk is likely to change over time. The link between one risk and others is also important. In particular, it is crucial to recognise the extent to which any risk involves a concentration with or can act as a diversifier to other risks.

In the same way that risk can mean different things to different people, so can enterprise risk management (ERM). The key concept here is the management of all risks on a holistic basis, not just the individual management of each risk. Furthermore, this should include both easily quantifiable risks such as those relating to investments and those which are more difficult to assess such as the risk of loss due to reputational damage.

A part of managing risks on a holistic basis is assessing risks consistently across an organisation. This means recognising both diversifications and concentrations of risk. Such effects can be lost if a 'silo' approach to risk management is used, where risk is managed only within each individual department or business unit. Not only might enterprise-wide concentration and diversification be missed, but there is also a risk that different levels of risk appetite might exist in different silos. The concept of risk appetite is explored in Chapter 15. Furthermore, enterprise-wide risks might not be managed adequately, with some risks being missed altogether due to a lack of ownership.

The term 'enterprise risk management' also implies some sort of process – not just the management of risk itself, but the broader approach of:

- recognising the context;
- identifying the risks;
- assessing and comparing the risks with the risk appetite;
- deciding on the extent to which risks are managed;
- taking the appropriate action; and
- reporting on and reviewing the action taken.

When formalised into a process, with detail added on how to accomplish each stage, then the result is an ERM framework. However, the above list raises another important issue about ERM: that it is not just a one-off event that is carried out and forgotten, but that it is an ongoing process with constant monitoring and with the results being fed back into the process.

It is important that ERM is integrated into the everyday way in which a firm carries out its business and not carried out as an afterthought. This means that risk management should be incorporated at an early stage into new projects. Such integration also relates to the way in which risks are treated since it recognises hedging and diversification, and should be applied at an enterprise rather than a lower level.

Moreover, ERM requires the presence of a central risk function (CRF), headed by a chief risk officer. This person should be responsible for all things risk-related,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

and in recognition of his or her importance, the chief risk officer should have access to or, ideally, be a member of the board of the organisation.

Putting an ERM framework into place takes time and requires commitment from the highest level of an organisation. It is also important to note that it is not some sort of 'magic bullet', and even the best risk management frameworks can break down or even be deliberately circumvented. However, an ERM framework can significantly improve the risk and return profile of an organisation.

1.2 Why Manage Risk?

With all this discussion of ERM, it is important to consider why it might be desirable to manage risk in the first place. At the broadest level, risk management can benefit society as a whole. The effect of risk management failures in banking on the economy, as shown by the global liquidity crisis, gave a clear illustration of this point.

It could also be argued that risk management is what boards have been appointed to implement, particularly in the case of non-executive directors. This does not mean that they should remove all risk, but they should aim to meet return targets using as little risk as possible. This is a key part of their role as agents of shareholders. It is in fact in the interests of directors to ensure that risks are managed properly, since it reduces the risk of them losing their jobs, although there are remuneration structures that can reward undue levels of risk.

On a practical level, risk management can also reduce the volatility in an organisation's returns. This could help to increase the value of a firm, by reducing the risk of bankruptcy and perhaps the tax liability. This can also have a positive impact on a firm's credit rating and can reduce the risk of regulatory interference. Reduced volatility also avoids large swings in the number of employees required – thus limiting recruitment and redundancy costs – and reduces the amount of risk capital needed. If less risk capital is needed, then returns to shareholders or other providers of capital can be improved or, for insurance companies and banks, lower profit margins can be added to make products more competitive.

Improved risk management can lead to a better trade-off between risk and return. Firms are more likely to choose projects with the best risk-adjusted rates of return, and to ensure that the risk taken is consistent with the corporate appetite for risk. Again, this benefits shareholders.

These points apply to all types of risk management, but ERM involves an added dimension. It ensures not only that all risks are covered but also that they are covered consistently in terms of the way they are identified, reported and treated. Moreover, ERM also involves the recognition of concentrations and diversifications

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

arising from the interactions between risks. ERM therefore offers a better chance of the overall risk level being consistent with an organisation's risk appetite.

Treating risks in a consistent manner and allowing for these interactions can be particularly important for banks, insurers and even pension schemes, as this means that the amount of capital needed for protection against adverse events can be determined more accurately.

Also, ERM implies a degree of centralisation, and this is an important aspect of the process that can help firms react more quickly to emerging risks. Centralisation also helps firms to prioritise the various risks arising from various areas of an organisation. Furthermore, it can save significant costs if extended to risk responses. If these are dealt with across the firm as a whole rather than within individual business lines, then not only can this reduce transaction costs, but potentially offsetting transactions need not be executed at all. Going even further, ERM can uncover potential internal hedges arising from different lines of business that reduce or remove the need to hedge either risk.

Having a rigorous ERM process also means that the choices of response are more likely to be consistent across the organisation, as well as more carefully chosen.

Another important advantage of ERM is that it is flexible – an ERM framework can be designed to suit the individual circumstances of each particular organisation.

Sometimes, ERM processes are implemented in response to a previous risk management failure in an organisation. This does mean that there is an element of closing the stable door after the horse has bolted, and perhaps too great a focus on the risk that was faced rather than potential future risks. It might also lead to excessive risk aversion, although introducing a framework where none has existed is generally going to be an improvement.

A risk management failure in one's own organisation is not necessarily the precursor to an ERM framework. A high-profile failure in another firm, particularly a similar one, might prompt other firms to protect themselves against similar events. An ERM framework might also be required by an industry regulator, or by a firm's auditors or investors.

Furthermore, ERM can be used in a variety of contexts. It should be considered when developing a strategy for an organisation as a whole and within individual departments. Once it has been decided what an organisation's objectives are, the organisation must consider what risks might result in them not being achieved. The organisation must then consider how to assess and deal with the risks, considering the impact on performance both before and after treating the risks identified. Importantly, the organisation needs to ensure that there is a framework in place for carrying out each of these stages effectively.

Also, ERM can be used for developing new products or undertaking new projects by considering both the objectives and the risk that they will not be met. Here, it is

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

also possible to determine the levels of risk at which it is desirable to undertake a project. This is not just about deciding whether risks are acceptable or not; it is also about achieving an adequate risk-adjusted return on capital, or choosing between two or more projects.

Finally, ERM is also important for pricing insurance and banking products. This involves avoiding pricing differentials being exploited by customers, but also ensuring that premiums include an adequate margin for risk.

1.3 Enterprise Risk Management Frameworks

Enterprise risk management frameworks typically share a number of common features. The first stage in most frameworks is to assess the context in which it is operating. This means understanding the internal risk management environment of an organisation, which in turn requires an understanding of the nature of an organisation and the interests of various stakeholders. It is important to carry out this analysis so that potential risk management issues can be understood. The context also includes the external environment, which consists of the broader cultural and regulatory environment, as well as the views of external stakeholders.

Then, a consistent risk taxonomy is needed so that any discussions on risk are carried out with an organisation-wide understanding. This becomes increasingly important as organisations get larger and more diverse, especially if an organisation operates in a number of countries. However, whilst a consistent taxonomy can allow risk discussions to be carried out in shorthand, it is important to avoid excessive use of jargon so that a framework can be externally validated.

Once a taxonomy has been defined, the risks to which an organisation is exposed must be identified. The risks can then be divided into those which are quantifiable and those which are not, following which the risks are assessed. These assessments are then compared with target levels of risk – which must also be determined – and a decision must be taken on how to deal with risks beyond those targets. Finally, there is implementation, which involves taking agreed measures to manage risk.

However, it is also important to ensure that the effectiveness of the approaches used is monitored. Changes in the characteristics of existing risks need to be highlighted, as do the emergence of new risks. In other words, risk management is a continual process. The process also needs to be documented. This is important for external validation, and for when elements of the process are reviewed. Finally, communication is important. This includes internal communication to ensure good risk management and external communication to demonstrate the quality of risk management to a number of stakeholders.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

1.4 Corporate Governance

Corporate governance is the name given to the process of running an organisation. It is important to have good standards of corporate governance if an ERM framework is to be implemented successfully. Corporate governance is important not only for company boards, but also for any group leading an organisation. This includes the trustees of pension schemes, foundations and endowments. Their considerations are different because they have different constitutions and stakeholders, but many of the same issues are important.

The regulatory aspects of corporate governance are discussed in depth in Chapter 5, whilst board composition is described in Chapter 4. It is also worth noting that corporate governance forms the 'G' in ESG (environmental, social and governance). As such, it is also addressed as a risk in Chapters 7, 14 and 16. However, it is worth commenting briefly on what constitutes good corporate governance.

1.4.1 Board Constitution

The way in which the board of an organisation is formed gives the foundation of good corporate governance. Whilst the principles are generally expressed in relation to companies, analogies can be found in other organisations such as pension schemes.

A key principle of good corporate governance is that different people should hold the roles of chair and chief executive. The chief executive is responsible for running the firm whilst the chair is responsible for running the board. Indeed, the EU Capital Requirements Directive 2013/36/EU (CRD IV) and the EC Markets in Financial Instruments Directive 2004/39/EC (MiFID) from the European Commission require financial firms to be controlled by at least two individuals. There are also restrictions on combining the roles of chair and chief executive in CRD IV.

It can be argued that having an executive chair – that is, a combined chief executive and chair – ensures consistency between the derivation of a strategy and its implementation. Indeed, this argument is used in many public companies in the United States. However, since the board is intended to monitor the running of the firm, there is a clear potential conflict of interest if the roles of chief executive and chair are combined. For this reason, there is pressure even in the United States for the roles of chief executive and chair to be separated.

It is also good practice for the majority of directors to be non-executives. This means that the board is firmly focussed on the shareholders' interests. Ideally, the majority of directors should also be independent, with no links to the company beyond their role on the board. Furthermore, independent directors should be the sole members of committees, such as remuneration (sometimes known as

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

compensation), audit and nominations (sometimes known as appointments), where independence is important.

1.4.2 Board Education and Performance

Whilst the composition of the board is important, it is also vital that the members of the board perform their roles to a high standard. One way of facilitating this is to ensure that directors have sufficient knowledge and experience to carry out their duties effectively. Detailed specialist industry knowledge is needed only by executive members of the board – for non-executive directors, it is more important that they have the generic skills necessary to hold executives to account.

These skills are not innate, and new directors should receive training to help them perform their roles. It is also important that all directors receive continuing education so that they remain well-equipped, and that their performance is appraised regularly. To ensure that appraisals are effective, it is important to set out exactly what is expected of the directors. This means that the chair should agree on a series of goals with each director on appointment and at regular intervals. The chair's performance should be assessed by other members of the board.

1.4.3 Board Compensation

An important way of influencing the performance of directors is through compensation. Compensation should be linked to the individual performance of a director and to the performance of the firm as a whole. The latter can be achieved by basing an element of remuneration on the share price. Averaging this element over several periods can reduce the risk of short-termism.

A similar way of incentivising directors is to encourage or even oblige them to buy shares in the firm on whose board they sit.

1.4.4 Board Transparency

Good corporate governance implies transparency in dealings with stakeholders who include shareholders, regulators, customers and employees, to name but a few. This means sharing information as openly as possible, including the minutes of board meetings, as far as this can be done without the disclosure of commercially sensitive information.

1.4.5 Board Diversity

Diversity is an important consideration for boards. In this context, diversity means reflecting a broad range of experience, backgrounds and views. This should help

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

boards to think more broadly and expose ideas to greater scrutiny. It can also help an organisation if the composition of the board reflects the composition of the workforce and the customer base. In both cases, it can help to ensure that the board remains engaged with its key stakeholders.

1.5 Models of Risk Management

In an ERM framework, the way in which the department responsible for risk management – the CRF – interacts with the rest of the organisation can have a big impact on the extent to which risk is managed. The role of the CRF is discussed in more detail in Chapter 3, but it is worth exploring the higher level issue of interaction here first.

1.5.1 The 'Three Lines of Defence' Model

One common distinction involves classifying the various parts of an organisation into one of three lines of defence, each of which has a role in managing risk. The first line of defence is carried out as part of the day-to-day management of an organisation, for example, those pricing and selling investment products. Their work is overseen on an ongoing basis, with a greater or lesser degree of intervention, by an independent second tier of risk management carried out by the CRF, supplemented by the compliance function. Finally, both of these areas are overseen on a less frequent basis by the third tier, audit.

This model explains the division of responsibilities well. However, it leaves open the degree of interaction between these different lines, in particular the first and second.

1.5.2 The 'Offence and Defence' Model

One view of the interaction of the first-line business units and the CRF is that the former should try and take as much risk as it can get away with to maximise returns, whilst the CRF should reduce risk as much as possible to minimise losses. This is the offence and defence model, where the first and second lines are set up in opposition.

The results of such an approach are rarely optimal. There is no incentive for the first-line units to consider risk, since they regard this as the role of the CRF. Conversely, the CRF has an incentive to stifle any risk-taking – even though taking risk is what an organisation must often do to gain a return.

It is better for first-line units to consider risk whilst making their decisions. It is also preferable for the CRF to maximise the effectiveness of the risk budget rather

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

than to try to minimise the level of risk taken. This means that whilst the offence and defence model might reflect the reality in some organisations, it should be avoided.

1.5.3 The Policy and Policing Model

A different approach involves the CRF setting risk management policies and then monitoring the extent to which those policies are complied with. This avoids the outright confrontation that can arise in the offence and defence model, but is not an ideal solution.

The problem with this approach is that it can be too 'hands-off'. To be effective, it is essential that the CRF is heavily involved in the way in which business is carried out, and this model might lead to a system that leaves the CRF too detached.

1.5.4 The Partnership Model

This is supposed to be the way in which a CRF interacts with the first-line business units, with each working together to maximise returns subject to an acceptable level of risk. It can be achieved by embedding risk professionals in the first-line teams and ensuring that there is a constant dialogue between these teams and the CRF.

However, even this approach is not without its problems. In particular, there is the risk that members of the CRF will become so involved in managing risk within the first-line units that they will no longer be in a position to give an independent assessment of the risk management approaches carried out by those units. The degree to which the CRF and the first-line units work together is therefore an important issue that must be resolved.

1.6 The Risk Management Time Horizon

Risk occurs because situations develop over time. This means that the time horizon chosen for risk measurement is important.

The level of risk over a one-year time horizon might not be the same as that faced after ten years – this is clear. However, as well as considering the risk present over a time horizon in terms of the likelihood of a particular outcome at the end of that period, it is also important to consider what might happen in the intervening period. Are there any significant outflows whose timing might cause a solvency or a liquidity problem?

It is also important to consider the length of time it takes to recover from a particular loss event, either in terms of regaining financial ground or in terms of reinstating protection if it has been lost. For example, if a derivatives counterparty fails, how long will it take to put a similar derivative in place – in other words, for how long must a risk remain uncovered?

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002

Finally, the time horizon itself must be interpreted correctly. For example, Solvency II – a mandatory risk framework for insurance companies – requires that firms have a 99.5% probability of solvency over a one-year time horizon. However, this is sometimes interpreted as being able to withstand anything up to a one-in-two-hundred-year event. Is this an accurate interpretation of the solvency standard? Would one interpretation be modelled differently from the other? All of these questions must be considered carefully.

1.7 Further Reading

There are a number of books that discuss approaches to ERM and the issues that ought to be considered. Lam (2003) and Chapman (2006) give good overviews, whilst McNeil et al. (2005) concentrate on some of the more mathematical aspects of ERM.

It is also important to remember that risk management frameworks can be used to gain an understanding of the broader risk management process. This is particularly true of the advisory risk frameworks such as International Organization for Standardization (2009).

Questions on Chapter 1

1. Describe why a firm with a large number of employees in a regulated industry might want to manage risk.
2. Describe the attractions of ERM as a way of managing risks in an organisation.
3. Give reasons for and against separating the roles of chair and chief executive.
4. State four models of risk management.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 06:55:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009565547.002