CFA Institute
Investment Foundations

A CLEAR UNDERSTANDING OF THE INDUSTRY

IS CFA INSTITUTE INVESTMENT FOUNDATIONS RIGHT FOR YOU?

Investment Foundations is a certificate program designed to give you a clear understanding of the investment management industry. Whether you're just starting a career in financial services or want to learn essential industry concepts, Investment Foundations offers an accessible solution for breaking through the complexities of the global investment industry and raising your professional profile.

THE BIG PICTURE

Investment Foundations is a comprehensive global education certificate program that provides a clear understanding of investment industry essentials. The certificate program is designed for all professional disciplines outside of investment roles, including IT, operations, accounting, administration, and marketing. There is no education or experience requirement and the exam can be taken at your convenience at available test centers around the world.

WHAT YOU LEARN

The certificate program covers the essentials of the investment management industry:

- **Module 1:** Industry Overview
- **Module 2:** Ethics and Regulation
- **Module 3:** Inputs and Tools
- **Module 4:** Investment Instruments
- **Module 5:** Industry Structure
- **Module 6:** Serving Client Needs
- **Module 7:** Industry Controls

HOW WILL YOU BENEFIT

Clarity
Benefit from having a common understanding of industry structure and terminology, regardless of your job function or geographic location.

Collaboration
Work more effectively with global colleagues by understanding industry functions, building stronger relationships and raising your professional competence.

Confidence
Gain the knowledge to identify issues and the confidence to speak up. Get a better sense of your role and how you connect with the complex global industry at large.

"[CFA Institute Investment Foundations] is very relevant to the current market and I can study on the move. The program cleared up a lot of concepts for me and now I am much more comfortable speaking with clients about what is happening in the market."

MITALI BHANDARE
MORNINGSTAR,
INVESTMENT FOUNDATIONS
CERTIFICATE HOLDER

"The main benefit of [CFA Institute Investment Foundations] was an ability to see a bigger picture of the finance industry and the role of our business within it."

ALEXANDER TARASOV
CITCO FUND SERVICES,
INVESTMENT FOUNDATIONS
CERTIFICATE HOLDER

HOW TO FIND OUT MORE

Go to: cfa.is/InvFound

www.cfainstitute.org

CHAPTER 18

RISK MANAGEMENT

by Hannes Valtonen, CFA

LEARNING OUTCOMES

After completing this chapter, you should be able to do the following:

a Define risk and identify types of risk;

b Define risk management;

c Describe a risk management process;

d Describe risk management functions;

e Describe benefits and costs of risk management;

f Define operational risk and explain how it is managed;

g Define compliance risk and explain how it is managed;

h Define investment risk and explain how it is managed;

i Define value at risk and describe its advantages and weaknesses.

INTRODUCTION 1

Risk is part of your daily life, and whether you realise it or not, you often act as a risk manager. Before crossing a busy road, you first assess that it is safe for you to do so; if you take a toddler to the swimming pool, you make sure that she is wearing inflatable armbands before she gets into the water and that she is never left unattended; you have probably purchased car, home, and/or health insurance to protect you and your family against accidents, disasters, or illnesses. Thus, in the course of your life, you are well acquainted with identifying risks, assessing them, and selecting the appropriate response, which is what risk management is about.

This chapter puts the emphasis on the types of risks that companies in the investment industry (investment firms) and people working for these companies face. It is important for companies to develop a structured process that helps them recognise and prepare for a wide range of risks. Although risk management is sometimes viewed as a specialist function, a good risk management process will encompass the entire company and filter down from senior management to all employees, giving them guidance in carrying out their roles. Any action that you take as an employee may affect your company's risk profile, even if these actions are "only" regular daily activities. An unintentional error can cause substantial damage to a company, so it is important that you gain a good understanding of the types of risks companies in the investment industry face and that you learn how these risks are managed.

DEFINITION AND CLASSIFICATION OF RISKS 2

Risk can take different forms. Although there is no universal classification of risks, this section identifies typical risks to which companies in the investment industry are exposed.

2.1 Definition of Risk

Risk arises out of uncertainty. It can be defined as the effect of uncertain future events on a company or on the outcomes the company achieves. One of these outcomes is the company's profitability, which is why the effects of risk on profit and rates of return are often assessed.

Events that have or could have a negative effect, leading to losses or negative rates of return, tend to be emphasised in discussions of risk. Some of these events are external to the company. For example, a bank that has a large portfolio of commercial loans may suffer substantial losses if the economy goes into recession and corporate defaults increase. Other events, such as internal fraud or network failure, are internal to the company. But not all outcomes from events are negative. Some events can have a positive effect on the company, creating opportunities for gains. For example, a company that takes the risk of investing in a country with tight capital controls (or controls on flows in financial markets) may benefit if the capital controls are lifted and the company becomes one of the few foreign companies licensed to buy and sell securities in that country. So, the assessment of risk needs to include opportunities as well as threats.

2.2 Classification of Risks

Risks are classified according to the source of uncertainty. There is a long list of sources of uncertainty, so there is a correspondingly long list of risks. Relatively well-defined categories of risk exist, but no standard risk classification system applies to all companies because risks should be classified in a manner that helps managers make better decisions in the context of their particular company and its environment.

All companies face the risk of not being able to operate profitably in a given competitive environment, typically because of a shift in market conditions. For example, a company's ability to grow and remain profitable may be affected by changes in customer preferences, the evolution of the competitive landscape, or product and technology developments.

There are three risks to which companies in the investment industry are typically exposed and that are discussed in this chapter:

- **Operational risk**, which refers to the risk of losses from inadequate or failed people, systems, and internal policies and procedures, as well as from external events that are beyond the control of the company but that affect its operations. Examples of operational risk include human errors, internal fraud, system malfunctions, technology failure, and contractual disputes.
- **Compliance risk**, which relates to the risk that a company fails to follow all applicable rules, laws, and regulations and faces sanctions as a result.
- **Investment risk**, which is the risk associated with investing that arises from the fluctuation in the value of investments. Although it is an important risk for investment professionals, it is less important for individuals involved in support activities, so it receives less coverage than operational and compliance risks in this chapter.[1]

1 Investment risks are discussed elsewhere in the curriculum. It was introduced in the Quantitative Concepts chapter and discussed further in the Investment Management chapter.

THE RISK MANAGEMENT PROCESS 3

A good risk management process helps companies reduce the likelihood and severity of adverse events and enhance management's ability to realise opportunities. The consequences of inadequate risk management include investment losses and even bankruptcy. Other costly consequences are also possible, such as sanctions for the breach of regulations, loss of licenses to provide financial services, and damage to the company's reputation and the reputations of its employees.

A risk management process provides a framework for identifying and prioritising risks; assessing their likelihood and potential severity; taking preventive or mitigating actions, if necessary; and constantly monitoring and making adjustments. A company's risk management process is not always consistently planned; it often evolves in response to crises, incorporating the lessons learned and the new regulatory requirements that sometimes follow these crises. Well-run companies, however, benefit from people and processes that enable forward-looking attention to emerging risks.

3.1 Definition of Risk Management

Risk management is a process—that is, a series of actions to achieve a company's objectives.[2] These objectives may take different forms, but they are typically driven by a company's mission and strategy. A common corporate objective is to create value in a business environment that is usually fraught with uncertainty. So, an important objective of the risk management process is to help managers deal with this uncertainty and identify the threats and opportunities their company faces. One of the main functions of risk management is to find the right balance between risk and return. Shareholders in a company or investors in a fund have invested their money for the promise of a return at some risk level. By limiting the effect of events that may derail the company's ability to achieve its objectives while benefiting from opportunities to grow the company profitably, risk management plays an important role in delivering value for these shareholders and investors.

The involvement of the board of directors and senior management in risk management is critical because they set corporate strategy and strategic business objectives. Although directors and senior managers are in charge of setting the appropriate level of risk to support the corporate strategy, risk management should involve all employees. One employee making an inaccurate or fraudulent assessment can damage the reputation of his or her company and even lead to its demise. Reputations take years to build but they can be lost in an instant. Markets are increasingly interdependent, and media and

2 The Committee of Sponsoring Organizations of the Treadway Commission (COSO), which provides guidance about risk management, internal control, and fraud deterrence, defines risk management as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". This definition is broad, but it highlights the key concepts associated with a risk management process. For more information, see *Enterprise Risk Management—Integrated Framework Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commission (September 2004): www.coso.org/documents/coso_erm_executivesummary.pdf.

the internet can spread the news of a mistake or scandal across the globe in a matter of minutes. Thus, risk management is critical to protecting reputations as well as maintaining confidence among market participants and trust in the financial system.

3.2 Steps in the Risk Management Process

A structured risk management process generally includes five steps, as illustrated in Exhibit 1.

Exhibit 1 Risk Management Process

3.2.1 *Set Objectives*

Setting objectives is an important part of business planning. Risk management enables management to identify potential events that could affect the realisation of those objectives. A company may set strategic objectives, which are typically high-level objectives connected to its mission. It may also define objectives that are related to its operations. Many of these objectives depend on external factors that may be difficult for companies to influence and control, which leads to a high degree of uncertainty. A strong risk management process helps decision makers ensure that the company is on track to achieve its objectives.

An important element in the setting of objectives is the company's risk tolerance. **Risk tolerance** is the level of risk that the company is able and willing to take on. The ability to handle risk is primarily driven by the company's financial health and depends on its level of earnings, cash flows, and equity capital. Its willingness to take on risk, which is also called its **risk appetite**, depends on its attitude toward risk and on its risk culture.

3.2.2 *Detect and Identify Events*

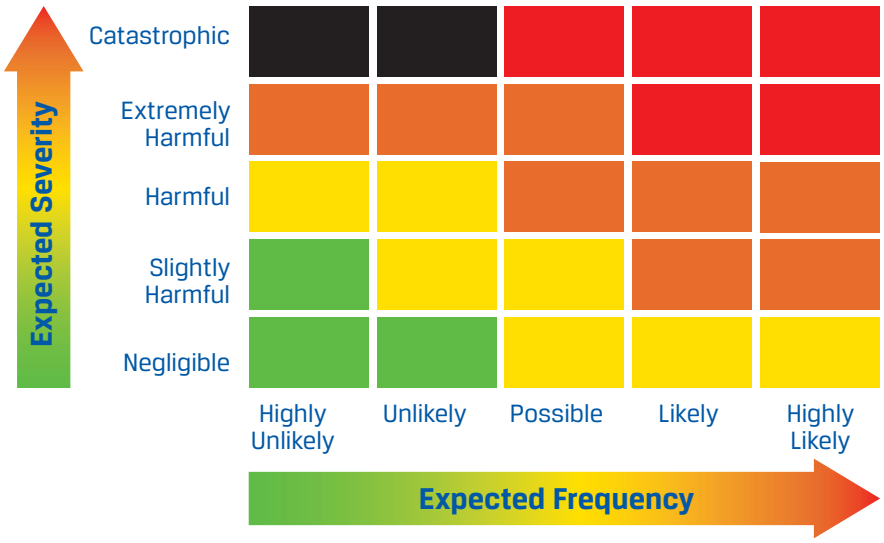
The next step in the risk management process is to detect and identify events that may affect achieving the company's objectives. As previously mentioned, the outcome of events can be negative—potentially leading to loss of earnings or assets—or they can be positive.

The aim of risk management is to try to capture the full range of risks, including hidden or undetected ones. Therefore, companies should involve employees in many different roles and business areas in order to detect and identify as many risks as possible. But there will always be unforeseen hazards. No matter how hard companies try to identify and reduce threats, they can never be completely identified or eliminated. The complexity of the business environment makes it impossible to understand and model the large number of possible outcomes and combinations of outcomes. What risk management provides is a robust framework to help companies prepare for adverse events, identify their occurrence as early as possible if they do materialise, and thus reduce their effect. The process of identifying potential risks can also reveal hidden value-enhancing opportunities.

3.2.3 *Assess and Prioritise Risks*

No matter what form risk takes, two elements of it are typically considered, in particular for undesirable events: the expected frequency of the event and the expected severity of its consequences. Different expected levels of frequency and severity of outcomes can be specified, as illustrated in Exhibit 2. This type of **risk matrix** can be used to prioritise risks and to select the appropriate risk response for each risk identified.

Exhibit 2 Risk Matrix



Depending on their expected level of frequency and severity, risks will receive different levels of attention:

- Green. Risks in the green area should not receive much attention because they have a low expected frequency and a low expected severity.
- Yellow. Risks coded yellow are either more likely but of low severity, or more severe but unlikely. They should receive a little more attention than risks in the green area, but less attention than risks in the orange area.
- Orange. Risks in the orange area have a higher expected frequency or higher expected severity than risks coded yellow, so they should be monitored more actively.
- Red. Risks coded red should receive special attention because they have a relatively high expected frequency and their effect on the company would be severe.
- Black. Risks in the black area are highly unlikely but would have a catastrophic effect. These risks are sometimes called "black swans", which is in reference to the presumption in Europe that black swans did not exist and is a belief that persisted until they were discovered in Australia in the 17th century. These risks are usually not identified until after they occur.

In practice, the selection of **key risk measures** is important for the risk management function to be proactive and predictive. Key risk measures should provide a warning when risk levels are rising. They require the collection and compilation of data from various internal and external sources. The types of key risk measures vary among industries and companies, and they need to be reviewed regularly to ensure that the measures are still relevant and sensitive to risk events.

Example 1 shows two of the many key risk measures that may be used by a securities brokerage firm. The example identifies the measure, the type of risk it is concerned with, the source of data, and how to interpret the measure.

EXAMPLE 1. TWO KEY RISK MEASURES USED BY A SECURITIES BROKERAGE FIRM

Key Risk Measure	Type of Risk	Source of Data	Interpretation
Client satisfaction index	Operational risk	Client surveys	A decrease in the client satisfaction index may be an indication that the quality of client services is deteriorating, which may have a negative effect on the firm's ability to generate revenue and profit.
Number of fines paid	Compliance risk	Legal or compliance department	An increase in the number of fines paid may be an indication that the firm does not comply with the required laws and regulations, which may result in the firm losing its ability to operate.

3.2.4 *Select a Risk Response*

The next step in risk management is to formulate responses to deal with the risks identified in the previous step. For each risk, management must select an appropriate response and develop actions to align the company's risk profile with its risk tolerance.

It is important to recognise that all companies must take risks in the course of their business activities to be able to create value. The restriction of activities to those that have no risk would not generate sufficient returns for shareholders or investors, who would thus be less willing to provide capital to companies or to invest their savings in the range of investments available.

Therefore, each company must determine the risks that should be exploited, which are often risks the company has expertise in dealing with and can benefit from. Companies must also determine the risks that should be mitigated or eliminated, which are often risks it has little or no expertise in dealing with. A risk management process that enables managers to distinguish between the risks that are most likely to provide opportunities and the risks that are most likely to be harmful helps companies generate superior returns. Risk response strategies can be classified into four "T" categories:

- *Tolerate.* This strategy involves accepting the risk and its effect. In some cases, the risk is well understood and taking it provides opportunities to create value. In other cases, the risk must be taken because other risk response strategies are unavailable or too costly.
- *Treat.* This strategy involves taking action to reduce the risk and its effect.
- *Transfer.* This strategy involves moving the risk and its effect to a third party.
- *Terminate.* This strategy involves avoiding the risk and its effect by ceasing an activity.

Example 2 illustrates the use of the four risk response strategies by a bank.

EXAMPLE 2. RISK RESPONSE STRATEGIES FOR A BANK

Assume that a bank has expertise in making loans to small companies in its home country. A neighbouring country is opening its economy and experiencing strong growth. The bank is looking for value-enhancing opportunities and decides to use its business expertise to make loans to small companies in the neighbouring country. At this stage, the bank is willing to *tolerate* the risks of doing business in a foreign country because the opportunity is potentially significant.

A few years later, the bank has a large portfolio of loans in the neighbouring country, but the economic situation there is deteriorating. The bank is concerned about the risk of an increasing number of borrowers defaulting on their loans; this risk is called credit risk and is discussed in Section 6.2. Thus, the bank decides to *treat* this credit risk by implementing stricter criteria before granting loans to small companies and by obtaining additional collateral to back each loan. Recall from the Debt Securities chapter that collateral refers to the assets that secure a loan.

The economic situation in the neighbouring country continues to deteriorate and the bank decides to *transfer* some of the credit risk to another financial institution that is willing to purchase part of the bank's portfolio of loans.

A few months later, the neighbouring country faces a recession, which leads to social and political unrest. The bank makes the decision that it no longer wants to do business there. It sells its remaining portfolio of loans to another financial institution and ceases all activities in the neighbouring country. In doing so, the bank *terminates* all risks.

In practice, investment firms set **internal risk limits** that incorporate the company's overall risk tolerance and risk management strategy—for example, by specifying the maximum amount of a risky security that can be held or the maximum aggregate exposure to one asset type or to one counterparty. Defining limits and then controlling and monitoring those limits allows firms to implement risk response strategies.

3.2.5 *Control and Monitor*

Taking action in response to risk involves a range of controlling and monitoring activities that must be performed in a timely manner. Policies and procedures provide a framework to help ensure that the risk responses are effectively implemented and monitored. Relevant information must be identified, captured, and reported accurately to enable people to carry out their responsibilities. Risk management, like many processes, should be iterative and subject to regular evaluations and revisions. Results must be used to make appropriate adjustments, which leads to a constant improvement in the risk management process.

At some point, risks must be consolidated and managed at the company level, bringing together different risks into an overall risk exposure. **Enterprise risk management (ERM)** helps a company manage all its risks together in an integrated way rather than managing each risk separately. The advantage of this approach is that it aligns risk management with objectives at all levels of the company, from the corporate level to the business unit level to the project level.

3.3 Risk Management Functions

If you process transactions, recruit people, manage information technology (IT) projects, or interact with clients, you are an integral component of your company's operations. Any failure to follow the appropriate policies and procedures may have a negative effect on your company.

Risk management functions vary by company, but it is typical for companies in the investment industry to have a stand-alone risk management function with a senior head, often called the chief risk officer, who is capable of independent judgment and action. The chief risk officer often reports directly to the board of directors. The purpose of establishing a strong independent risk management function is to build checks and balances to ensure that risks are seriously considered and balanced against other objectives, such as profitability.

Despite the existence of specialist risk managers, risk management remains everyone's responsibility. Risk managers assess, monitor, and report on risks, and in some cases, they may have an approval function or veto authority. But it is the members of the business functions, such as portfolio managers or traders, who "own" the risk of their deals. These employees have the most intimate knowledge of what they trade, and they must monitor their deals on a regular basis. The risk manager must ensure that all relevant risks are identified, but the final judgment on the business decision lies with the decision makers. Therefore, it is important for risk management to be part of the company's corporate culture and to be fully integrated with core business activities.

Companies will often use a three-lines-of-defence risk management model, as illustrated in Exhibit 3 below.

Exhibit 3 Three Lines of Defence

Front-line employees and managers, through their daily responsibilities, form the first line of defence. The risk management and compliance groups operate as a second line of defence, assisting and advising employees and managers while maintaining a certain level of independence. An internal audit function then forms the third line of defence. **Internal audit** is an independent function. Internal auditors follow risk-based internal audit programmes, delving into the details of business processes and ensuring

that information technology and accounting systems accurately reflect transactions. Proactive auditors may also advise managers on how to improve risk management, controls, and efficiency. Best practice suggests that internal auditors should report directly to the audit committee of the board of directors to ensure their independence. Thus, risk and audit committees of the board will often hear presentations from the heads of risk management, compliance, and internal audit.

3.4 Benefits and Costs of Risk Management

Risk management provides a wide range of benefits to a company. It can help by

- supporting strategic and business planning;
- incorporating risk considerations in all business decisions to ensure that the company's risk profile is aligned with its risk tolerance;
- limiting the amount of risk a company takes, preventing excessive risk taking and potential related losses, and lowering the likelihood of bankruptcy;
- bringing greater discipline to the company's operations, which leads to more effective business processes, better controls, and a more efficient allocation of capital;
- recognising responsibility and accountability;
- improving performance assessment and making sure that the compensation system is consistent with the company's risk tolerance;
- enhancing the flow of information within the company, which results in better communication, increased transparency, and improved awareness and understanding of risk; and
- assisting with the early detection of unlawful and fraudulent activities, thus complementing compliance procedures and audit testing.

All of these benefits should enhance the company's ability to create value.

The costs of establishing risk management systems include tangible costs, such as hiring dedicated risk management personnel, putting in place procedures, and investing in systems, and intangible costs, such as slower decision making and missed opportunities.

So, allocation of resources to risk management should be based on a cost–benefit analysis. It is difficult to weigh the costs and benefits of risk management precisely because it is impossible to observe, let alone measure, the cost of potential catastrophes that are averted. It is only in hindsight that the cost–benefit trade-offs can be identified. A case in point is Barings Bank's collapse in 1995, which was triggered by trading losses hidden in the bank's Singapore branch. At the time, there was no adequate and effective system for reconciling client orders and trades on a global basis. Such a system could have revealed the losses before they wiped out all of the bank's equity capital. It is estimated that implementing this system would have cost about £10 million, a small price to pay compared with the £827 million loss that brought down Barings.

OPERATIONAL RISK 4

As mentioned earlier, operational risk is the risk of losses from inadequate or failed people, systems, and internal policies and procedures, as well as from external events that are beyond the control of the company but that affect its operations.

4.1 Managing People

Human failures range from unintentional errors to fraudulent activities. Many companies are exposed to occupational fraud (sometimes called internal fraud or employee fraud), which is when an employee abuses his or her position for personal gain by misappropriating the company's assets or resources. In a survey carried out by the Association for Certified Fraud Examiners (ACFE), anti-fraud experts estimated that globally companies lose, on average, 5% of their annual revenues to fraud.[3]

One example of operational risk that has a human component and that is more frequent in the financial services industry than in any other industry is rogue trading. **Rogue trading** refers to situations wherein traders bypass management controls and place unauthorised trades, at times causing large losses for the companies they work for. Rogue trading may involve fraudulent trading that is done for personal enrichment or to make up losses. Exhibit 4 lists some of the largest rogue trading incidents.

Exhibit 4 Examples of Rogue Trading Incidents

Year of the Loss	Company	Rogue Trader	Estimated Loss
1995	Barings Bank	Nick Leeson	£827 million
1995	Daiwa Bank	Toshihide Iguchi	US$1.1 billion
1996	Sumitomo Corporation	Yasuo Hamanaka	¥285 billion
2002	Allied Irish Banks	John Rusnak	US$691 million
2004	National Australia Bank	Gianni Gray and others	AU$360 million
2004	China Aviation Oil	Chen Jiulin	US$550 million
2008	Société Générale	Jérôme Kerviel	€4.9 billion
2008	Groupe Caisse d'Epargne	Boris Picano-Nacci	€751 million
2011	UBS	Kweku Adoboli	$2.3 billion

Source: Thomas S. Coleman, *A Practical Guide to Risk Management* (Charlottesville, VA: Research Foundation of CFA Institute, 2011):91–92.

3 Information from http://www.acfe.com/press-release.aspx?id=4294973129.

Banks, like most companies, have tried to learn from past events and plug the holes in their systems and controls to prevent similar events from occurring. The failure of Barings Bank in 1995 revealed the danger of not segregating front and back office activities properly. In the small bank branch of Barings in Singapore, the same individuals managed both types of activities. An initial trading loss (a front office activity) because of a human error was hidden in the accounting system (a back office activity), and subsequent losses accumulated until they exceeded the bank's equity capital. Following Barings' collapse, banks were required to establish a clear separation between their front and back offices.

Companies can mitigate operational risks through education, by clearly communicating policies and procedures and by having efficient and effective internal controls. Good human resource management processes are also critical; hiring the right people and motivating them with the right incentives are well-known ingredients for success.

To avoid the risk of recruiting the wrong people, companies typically take various precautions, such as the following:

- Carrying out background checks, such as checking criminal records and disciplinary records with regulators for new hires
- Verifying credentials and previous work experience
- Performing personality assessment tests
- Getting character references to confirm suitability

Although these precautions may appear to be standard, studies have shown that discrepancies between presented and actual credentials are common. Cases in which background checks of senior executives were not appropriately performed are regularly reported. Because of a loss of trust, some of these executives had to resign when the truth was revealed, even if they had performed successfully in their position.

Risk taking should also be considered in the structure of compensation, for example when defining bonus payments for employees. It is particularly important for employees who expose the company to significant risks, such as traders and investment staff. A good compensation system should take into account the level of risk undertaken for a given level of return and should reward those who achieve returns without taking excessive risks. An example of an incentive that could lead to perverse behaviour is rewarding traders for profits regardless of the risks they take. This approach would give them all the upside for trading gains, but less downside for taking on risks and trading losses. In practice, traders generating substantial losses typically lose their jobs and reputations, but they usually do not have to pay back much compared with the compensation they previously received. Some authorities are now imposing new compensation structures that include deferred compensation to take into account long-term performance as well as claw-back provisions, whereby employees may have to return their bonuses if reported profitable deals result in losses later.

4.2 Managing Systems

Companies rely heavily on information technology (IT) systems. Consequently, technology has become an increasingly important source of operational risk. Automated processes can reduce the frequency and severity of operational errors, but they are not infallible. Failures of IT and communication systems can paralyse business operations or greatly reduce their efficiency, harming the company's profitability via lower revenues, higher costs, or a combination of both.

IT networks are inherently vulnerable to disruptions and outside interference because of technical limitations and human factors. One source of risk is the behaviour of employees who do not follow internal policies and, for instance, download unauthorised applications for personal or business use. The dangers of this practice include malicious viruses and unlicensed, and perhaps incompatible, software getting into company systems. In addition, IT departments are in a constant battle with hackers who exploit weaknesses to penetrate systems. Key controls to protect systems and business information include the establishment and communication of internal policies for users and IT technical staff, the creation of appropriate security standards and configurations for systems, and the allocation of adequate personnel and technical resources to maintain a well-controlled IT environment.

The protection of confidential information is also important in the investment industry. Data privacy has received a great deal of prominence recently because of a number of cases in which companies and government agencies have allowed people's private information to enter the public domain, exposing them to the risk of fraud. A company should understand how data are produced and flow internally, classify the information by sensitivity, assess the risks of data loss, and adopt appropriate preventative measures. Many countries have strict laws and regulations for protecting customer data, along with severe penalties for violating these laws and regulations.

4.3 Complying with Internal Policies and Procedures

The structure of a company varies with size and business activities engaged in, but there are features common to all companies. For instance, power and authority are delegated and responsibilities are assigned within most companies. In smaller entrepreneurial companies, such assignments may be communicated informally, with employees understanding their individual roles and degrees of authority. In larger and more complex companies, the roles and levels of authority will be formally defined and the business processes mapped out in more detail, usually embedded in corporate management systems. Policies and procedures should explicitly set out the delegation of authority and define clear responsibilities and accountability. These definitions form the basis for the monitoring of and control over business processes and provide feedback mechanisms.

The segregation of duties is an important principle that international companies and regulators and other authorities in many countries require and recommend. As mentioned earlier, a clear separation needs to exist between front and back offices. In accounting departments, there should also be a clear separation between those who enter items into the accounts and those who reconcile the bank statements with the cash balances in the accounting system. This separation of roles reduces the risk that employees who control cash will commit fraud or embezzle funds.

Compliance and internal audit functions are key to ensuring that employees are actually following internal policies and procedures.

4.4 Managing the Environment

The type of environment in which a company operates can add layers of uncertainty that need to be addressed.

4.4.1 *Political Risk*

Political risk is the risk that a change in the ruling political party of a country will lead to changes in policies that can affect everything from monetary policy (money supply, interest rates, and credit) and fiscal policy (taxation) to investment incentives, public investments, and procurement. Some industries are heavily influenced by governments that, for example, control natural resources or set prices of raw material inputs or products. In these instances, a change in administration or policies can affect the value of an investment. Political risk is inherent in all countries and should always be considered, even if it is perceived to be relatively remote.

4.4.2 *Legal Risk*

Legal risk is the risk that an external party will sue the company for breach of contract or other violations. A company should consider how it identifies and conforms to all legal commitments it has undertaken.

The role of an in-house legal expert is crucial to controlling legal risk. Most areas of a company have dealings with external parties, such as deal counterparties, business partners, suppliers, and service providers. An important control in managing the legal risk of these external relationships is to have legal experts review every contract. Companies should clearly delegate authority and specify who should review and approve which type of contracts. The most significant deals usually require approval at the level of the board of directors. Another control is to use template agreements and standard contract terms and conditions that have been reviewed and approved by the legal team.

The storage of records, documents, and all forms of communication must also be in line with legal requirements for all relevant jurisdictions, a topic that will be discussed in the Investment Industry Documentation chapter.

4.4.3 *Settlement Risk*

Settlement risk (or counterparty risk) is the risk that when settling a transaction, a company performs one side of the deal, such as transferring a security or money, but the counterparty does not complete its side of the deal as agreed, often because it has declared bankruptcy. This risk is sometimes also called Herstatt risk because of an incident in 1974 when the German Herstatt Bank ceased operations after counterparties had honoured their obligation to transfer Deutsche Marks to Herstatt, but before Herstatt honoured its obligation to transfer the equivalent amount in US dollars back to these counterparties.

Although there are usually legal means to compel a counterparty to perform its obligations, such measures are costly and time-consuming. A counterparty is more likely to find it difficult to fulfil its obligations during challenging economic times or when bankruptcy is imminent than during profitable times. In the case of bankruptcy, it may take months or years to receive assets through a bankruptcy resolution procedure and the proceeds may only be a fraction of the original nominal amount of debt.

It is important to distinguish the risks inherent in bilateral arrangements from those in transactions contracted through central counterparties, such as clearing houses. As discussed in the Structure of the Investment Industry chapter, clearing houses may step in to assume the risk of a counterparty failing to meet its contractual obligations. Other arrangements to reduce this risk are margin requirements, discussed in the Derivatives chapter, or standardised agreements.

COMPLIANCE RISK 5

Compliance risk is the risk that a company fails to comply with all applicable rules, laws, and regulations. The risk of non-compliance with laws and regulations is higher than non-compliance with internal policies and procedures because sanctions can be applied. These sanctions can affect both individuals and companies and may be severe. Ensuring compliance with rules and regulations has often been viewed as a rather mundane chore, but the rapidly changing regulatory environment has recently brought compliance to the forefront of business priorities. Many people believe that the trend toward less regulation contributed to the global financial crisis that began in 2008. The trend has reversed with the re-imposition of greater regulation and oversight. This increased legislation, in turn, has led to more compliance activities and more compliance risk.

5.1 Framework for Legal and Regulatory Compliance

Every company has to follow a set of rules, beginning with the statutory laws and other regulations imposed by regulatory bodies. In addition, many investment firms must follow guidelines from regulators, stock exchanges, and industry associations that have been given powers to oversee members. Because of their importance in the financial system, banks and insurance companies have historically been subject to heavy regulation, with detailed rules and scrutiny from regulatory authorities. For example, banks are subject to the Basel Accords. Accords are international agreements that usually take the name of the location where they are signed. The Basel Accords, which define international standards regarding banks' capital, leverage, and liquidity requirements, are discussed on a regular basis in Basel, Switzerland. As of May 2014, the latest version of these accords is Basel III.

Complying with applicable laws and regulations is required of every company. The consequences of not doing so can be severe and can include financial penalties, loss of business licenses, lawsuits by clients, and in serious cases, prison terms. Often the greatest consequences are the damage to the company's reputation and the loss of existing and potential business opportunities.

Companies should have internal reporting procedures to encourage employees to come forward and report instances in which they suspect someone has violated internal policies, procedures, laws, or regulations. This process is called whistle-blowing. Whistle-blowing has become an important way for authorities to learn of violations, and provisions to protect and reward whistle-blowers have been strengthened in the wake of financial scandals.

5.2 Example of Key Compliance Risks

Types of regulation and how to comply with them are outlined in the Regulation chapter. Below are just a few examples of key compliance risks that have the potential to inflict serious damage on investment firms and their employees.

5.2.1 *Corruption*

Corruption, which is defined as the abuse of power for private gain, has received heightened attention because of tightened laws and regulations on bribery and increased regulatory scrutiny, investigations, prosecutions, and fines. Some national authorities may apply these laws extra-territorially, even to foreign entities. Firms that operate through agents and other third parties should be aware that their responsibility for preventing corruption extends to the actions of these third parties. Ignoring the practices of third parties does not constitute a defence in the event of a regulatory investigation.

To safeguard against corruption, companies must start by establishing a tone at the top, with senior management communicating an unambiguous policy of zero tolerance for unethical business practices and bribery. Risk assessments should identify major risk areas and susceptible employees. For instance, employees who deal with government officials for licensing or deal with government or state-owned entities should be given enhanced training and be monitored closely. Controls over corporate gifts and hospitality, especially in payment-processing areas, are crucial for the prevention of illegal or unethical payments.

5.2.2 *Tax Reporting*

Compliance with tax regulations is complicated because the principles and rules vary considerably by jurisdiction. Companies are continuously developing financial and legal structures, often with the intention of minimising taxes overall. Uncertainty exists in how tax authorities will apply their rules, which is compounded by the fact that rules change regularly. A conservative approach is to conform to tried-and-tested precedents. A more aggressive approach is to seek to exploit loopholes in the tax code, low-tax jurisdictions (so-called offshore tax havens), and other grey areas.

There is a technical difference between "tax avoidance", which means using tax code provisions to minimise the tax that is owed, and "tax evasion", which means not paying taxes in violation of the tax law. In practice, however, the line between tax avoidance and tax evasion is not always clear and expert tax advice is necessary. From a risk-management perspective, tax risk should be managed in a consistent manner, incorporating the appropriate expertise at each stage of a transaction or financial reporting cycle.

5.2.3 *Insider Trading*

There are laws that prohibit the trading of a security when in possession of important confidential information pertaining to the security in question. Most markets have recently tightened laws regulating insider trading. Another trend is an increase in investigations of insider trading; some such investigations are even relying on techniques similar to those used in investigations of organised crime cases—including tapping telephones, using evidence already collected to make peripheral suspects co-operate, and gradually closing in to catch the central participants of the scheme. Companies must implement policies and procedures to ensure that traders understand the laws and that nobody in the company will be in the position to violate them. Investment firms that face a high risk of insider trading, such as investment banks, have "control rooms" to monitor information flowing between teams. They also have virtual walls or information barriers to restrict and segregate information and to manage other conflicts of interest. These virtual walls are sometimes called Chinese walls, which may be in reference to the screens that were common in China to separate large areas into smaller rooms or in reference to the Great Wall of China.

5.2.4 *Anti-Money-Laundering*

Anti-money-laundering legislation is a set of rules to prevent money derived from criminal activities from entering the financial system and acquiring the appearance of being from legitimate sources. These rules require companies in the financial services industry, including those in the investment industry, to obtain sufficient original or certified documentation to perform a formal risk assessment on each client and counterparty; the procedures of such an assessment are called know-your-customer procedures.

International agreements defining basic principles and requirements for anti-money-laundering frameworks have been developed and are implemented with slight variations according to the jurisdiction. A notable feature of most anti-money-laundering regulation is a strict liability approach to compliance. That is, a company can be subject to severe sanctions as a result of not following required procedures and record keeping, regardless of whether any suspicious transactions are handled or any actual damage is caused.

INVESTMENT RISK 6

Risk is a critical element of investment decisions. Investors, for instance, buy equity securities, commodities, or real estate. When they do, they are exposed to investment risk—that is, the risk associated with investing. For example, investors may face losses if the company in which they bought common shares loses value or goes bankrupt or if commodity or real estate prices fall.

Investment risk can take different forms depending on the company's investments and operations. Companies in the investment industry typically experience three broad types of investment risk:

- **Market risk**, which is the risk caused by changes in market conditions affecting prices.
- **Credit risk**, which is the risk for a lender that a borrower fails to honour a contract and make timely payments of interest and principal.
- **Liquidity risk**, which is the risk that an asset or security cannot be bought or sold quickly without a significant concession in price.

A common theme for success in all types of investment risk management is the need to understand the risks and price them accurately.

6.1 Market Risk

Market risk, which arises from price movements in financial markets, can be classified into the risks associated with the underlying market instruments: equity price risk, interest rate risk (for debt securities), foreign exchange rate risk, and commodity price risk.

Many investment firms are in the business of assuming investment risks, and they tend to tolerate market risks. But like any other company, they must align their risk profiles with their risk tolerance. They often implement an approach called **risk budgeting** to determine how risk should be allocated among different business units, portfolios, or individuals. For example, an asset management firm may use the following risk budgeting steps:

- Quantify the amount of risk that can be taken by the firm
- Set risk budgets and limits for each asset class and/or investment manager
- Allocate assets in compliance with the risk budgets
- Monitor to ensure that risk budgets are respected

Market risks that cannot be tolerated must be mitigated, and companies have different alternatives available. One of them is to hedge unwanted risks by using derivative instruments. The Derivatives chapter and Economics of International Trade chapter offer examples of how companies can hedge unwanted risks.

6.2 Credit Risk

When assessing the creditworthiness of borrowers, it is important to consider both their ability and willingness to repay their debts. For example, after the fall in real estate prices in 2008, many homeowners in the United States were left with mortgage loan balances that exceeded the market value of the property. Some of those borrowers still had the ability to keep paying their mortgage loans but decided to default

and let the bank take possession of the property. This potentially unethical decision is rational from a purely financial perspective, apart from the worse credit profile for future borrowing.

The expected loss from credit exposure is a function of three elements: the amount of money lent to a particular borrower, the probability that the borrower defaults, and the loss that would be incurred if the borrower defaults. The amount that is at risk may be reduced if collateral or guarantees from third parties are included. Enforcing contract provisions to take possession of collateral, however, can be a time-consuming legal process. The value of collateral assets for a lender depends on their liquidity and marketability—that is, how easy it is to sell the assets to a third party and at how much of a discount if sold on short notice. Assets for which a steady market demand exists and that can be moved and easily transferred are more valuable than assets that are traded less frequently and are less mobile.

Various sources of independent information exist on borrower creditworthiness, such as credit rating agencies, which should be used in conjunction with internal risk analysis. Any analysis, whether internal or external, should involve a degree of critical judgment and scepticism.

There are various approaches to managing credit risk, including the following:

- Set limits on the amount of exposure to a particular counterparty or level of credit rating allowed. For example, a maximum limit of 5% exposure could be set for a particular counterparty.
- Require additional collateral and impose covenants. Covenants, discussed in the Debt Securities chapter, are terms for loans that specify both what a borrower must do (positive covenants) and what a borrower is not allowed to do (negative covenants). For example, a bank may restrict borrowers from issuing more debt, paying dividends, or entering into highly risky business ventures. When one of the restrictive conditions is broken, the lender may recall the loan or demand some action, such as the assignment of additional collateral.
- Transfer risk by using derivative instruments. Credit default swaps are often used when companies want to protect themselves against the risk of a loss in value of a debt security or index of debt securities, as discussed in the Derivatives chapter.

Lending to governments or state-owned companies creates another type of credit risk. **Sovereign risk** is the risk that a government will not repay its debt because it does not have either the ability or the willingness to do so. The unique aspect of sovereign risk is that lenders have limited legal remedies available to compel the borrower to repay or to be able to recover the assets themselves. A government can also prevent borrowers in its country from repaying their debts to foreign investors—for example, by implementing currency controls to make it difficult or impossible for money to leave the country.

6.3 Liquidity Risk

Liquidity refers to the ability to buy and sell quickly without incurring a loss. It is a core concern for companies and is often neglected when sources of financing, such as bank credit, are plentiful. But during the global financial crisis of 2008, an acute shortage of liquidity in the financial systems in many countries led to failures. These failures occurred because some companies were unable to maintain access to sufficient money to finance their working capital (inventories and receivables from customers net of payables from suppliers) and, therefore, to keep their companies going.

Firms in the investment industry face a greater level of liquidity risk than, say, manufacturers. To operate profitably, they need markets that can accommodate their trades without significant adverse effects on prices. When markets are illiquid—either temporarily, such as during financial crises, or more structurally, such as in some emerging markets—the ability to trade assets is substantially reduced, which has a negative effect on these firms.

7 VALUE AT RISK

Companies in the financial services industry expect that the assets and securities they hold will provide them with a positive return. However, they also need to estimate the potential loss on an investment if their forecasts for the asset or security turn out to be inaccurate. This potential loss is often measured using a metric known as value at risk.

7.1 Use and Advantages of Value at Risk

Value at risk (VaR) was developed in the late 1980s and is now a widely used metric. It relies on some of the statistical concepts, such as standard deviation, discussed in the Quantitative Concepts chapter. VaR gives an estimate of the minimum loss of value that can be expected for a given period with a given level of probability. For example, an asset management firm may estimate that a portfolio has a VaR of $1 million for one day with a probability of 5%. This means that there is a 5% chance that the portfolio will fall in value by at least $1 million in a single day, assuming no further trading. Put another way, a loss of $1 million or more for this portfolio is expected to occur, on average, once in 20 trading days (1/0.05).

VaR offers several advantages:

- It is a standard metric that can be applied across different investments, portfolios, business units, companies, and markets.
- It is relatively easy to calculate and well understood by senior managers and directors.
- It is a useful tool for risk budgeting if there is a central process for allocating capital across business units according to risk.
- It is widely used and mandated for use by some regulators.

7.2 Weaknesses of VaR

There are also weaknesses inherent in the VaR measure of risk. VaR gives an estimate of the minimum, but not the maximum, loss of value that can be expected. Referring back to the earlier example, the asset management firm can expect a loss of at least $1 million 12 or 13 times a year (5% of the approximately 250 trading days a year). VaR does not indicate the maximum loss of value the portfolio manager can expect to bear in one day, and it does not guarantee that a loss in excess of $1 million will not happen more frequently than a dozen times a year.

In practice, VaR often underestimates the frequency and magnitude of losses, mainly because of erroneous assumptions and models. First, VaR primarily relies on historical data to forecast future expected losses. But past returns may not be a good predictor of future returns. In addition, history is not helpful in forecasting events that have far-reaching effects, but are unforeseen or considered impossible—that is, black swan events. Second, VaR makes an assumption regarding the distribution of returns. For example, it is often assumed that returns are normally distributed and follow the bell-shaped distribution presented in Exhibit 8 in the Quantitative Concepts chapter. The use of historical data and the assumption of a normal distribution may work relatively well in normal market conditions but not during periods of market turmoil.

The global financial crisis of 2008 is a case in point. Until 2007, most banks had a low daily VaR, which gave them a false sense of security. Once the crisis hit, the number of days when trading losses exceeded the daily VaR and the amount of those losses were substantially higher than predicted. Some banks reported that the frequency of losses was 10 to 20 times higher than the VaR predictions, and some banks recorded losses that significantly reduced their equity capital.

To address these weaknesses, companies—in particular, banks—often use complementary risk management techniques in addition to VaR. These complementary techniques include scenario analysis and stress testing, which focus on the effect of more extreme situations that would not be fully captured or evaluated with VaR. For example, an asset management firm may perform a scenario analysis by identifying different scenarios for the economy (strong growth, moderate growth, slow growth, no growth, mild recession, and severe recession) and then determining how each scenario would affect the value of a portfolio and the firm's earnings and equity capital. The firm may also engage in stress testing by examining the effect of extreme market conditions, such as a liquidity crisis, to make sure that it would be resilient and would survive the crisis.

It is worth noting that the weaknesses related to VaR apply to all measures that rely on models. The risk arising from the use of models is collectively known as **model risk**. This risk is associated with inappropriate underlying assumptions, the unavailability or inaccuracy of historical data, data errors, and misapplication of models.

SUMMARY

Although most companies in the investment industry have dedicated risk management functions, it is important to remember that risk is not just the responsibility of the risk management team—everyone is a risk manager. So, even if you are not a risk management specialist, you should still seek to understand risk management process, systems, and tools and participate in risk management activities in your organisation.

The points below recap what you have learned in this chapter about risk management:

- Risk is defined as the effect of uncertain future events on a company or on the outcome that the company achieves. Types of risks are often categorised according to the source of risk: operational risk, compliance risk, and investment risk. The latter category includes market risk, credit risk, and liquidity risk.
- Risk management is an iterative process that helps companies reduce the chances and effects of adverse events while enhancing the realisation of opportunities. This process includes five steps: setting objectives, detecting and identifying events, assessing and prioritising risks, selecting a risk response, and controlling and monitoring activities.
- Risk assessment involves the identification of undesirable events and the estimation of their expected frequency and the expected severity of their consequences. It is important for a company to build a risk matrix and select key risk measures to prioritise risks and warn when risk levels are rising.
- Risk response strategies include exploiting risks that the company has expertise dealing with and can benefit from as well as mitigating or eliminating risks that the company has little or no expertise in dealing with. Risk response strategies include tolerating, treating, transferring, or terminating risk.
- Companies often use a three-lines-of-defence risk management model, in which employees and managers form the first line of defence, the risk management and compliance groups operate as a second line of defence, and an internal audit function forms the third line of defence.
- Allocation of resources to risk management should be based on a cost-benefit analysis. Typical costs include tangible costs, such as hiring dedicated risk management personnel, putting procedures in place and investing in systems, and intangible costs, such as slower decision making and missed opportunities. Overall, risk management should have a positive effect on a company's ability to achieve its strategic objectives and improve its operations, ultimately leading to value creation.
- Operational risk is the risk of losses from inadequate or failed people, systems, and internal policies and procedures, as well as from external events that are beyond the control of the company but that affect its operations. The reduction of operational risk requires companies to manage people to reduce human

failures ranging from unintentional errors to fraudulent activities; manage systems, particularly IT and communication systems, and ensure compliance with internal policies and procedures; and manage political, legal, and settlement risks.

- Compliance risk is the risk that a company fails to comply with all applicable rules, laws, and regulations. The company may face sanctions and damage to its reputation as a result of non-compliance. Examples of key compliance risks that have the potential to inflict serious damage on investment firms and their employees include corruption, inadequate tax reporting, insider trading, and money laundering.

- Investment risks take different forms depending on the company's investments and operations. Investment firms typically experience: market risk, caused by changes in market conditions affecting prices; credit risk, caused by borrowers' inability and/or unwillingness to make timely payments of interest and principal; and liquidity risk, caused by difficulties in buying or selling assets or securities quickly without a significant concession in price.

- Value at risk, which provides an estimate of the minimum loss of value that can be expected for a given period of time with a given probability, is a widely-used metric to measure risk. By relying on historical data and making assumptions about the distribution of returns, VaR suffers from weaknesses that are typical of all measures that rely on models.