A practical guide to understanding and managing risk

MASTERING RISK MANAGEMENT

- Provides an invaluable framework for the management of risk
- Helps you identify, monitor and manage risk
- Shows you how to change your culture effectively
- Explains how you can lessen reputation damage
- Challenges modelling risk through a business approach

TONY BLUNDEN
JOHN THIRLWELL

FT PUBLISHING

About the book

Mastering Risk Management provides a step-by-step guide from basic to advanced elements of risk management.

Following a 3-part framework, it covers:

1. What do we mean by risk management?
2. How do you use risk management tools for business benefit?
3. What keeps management awake at night?

'Read this book to help understand that risk management is about both challenge and opportunity. This book helps you to navigate the perilous waters of business with tools and techniques to help you sleep at night.'

Mark Sismey-Durrant, Chairman, Cashplus Bank; Chair of the Strategy Advisory Board, Loughborough University School of Business and Economics

'Forewarned is forearmed. This masterpiece successfully navigates useful practical steps, tools, frameworks and techniques to manage, anticipate and address new and emerging risks while tackling existing ones. In today's world of risk and reward, this is a must read.'

Sir Peter Estlin, independent non-executive director of Rothschild & Co; Chair of FutureDotNow; former Lord Mayor of the City of London

Praise *for Mastering Risk Management*

'Here is a straightforward, no-nonsense guide to risk and its integral role in the management process. Using clear examples, Blunden and Thirlwell distil their insights on why respect for risk is a crucial success factor for business. Ignore it at your peril.'

Jane Platt, Chair of Zurich Assurance Ltd;
Chair of LifeSight by Willis Towers Watson;
former non-executive director of the FCA

'Forewarned is forearmed. This masterpiece successfully navigates useful practical steps, tools, frameworks and techniques to manage, anticipate and address new and emerging risks while tackling existing ones. In today's world of risk and reward, this is a must read.'

Sir Peter Estlin, independent non-executive director,
Rothschild & Co; Chair, FutureDotNow;
former Lord Mayor of the City of London

'Read this book to help understand that risk management is about both challenge and opportunity. This book helps you to navigate the perilous waters of business with tools and techniques to help you sleep at night.'

Mark Sismey-Durrant, Chairman, Cashplus Bank;
Chair, Strategy Advisory Board, Loughborough
University School of Business and Economics

'The events of 2020 and 2021 have caused everyone to consider their true readiness for the magnitude of "disruption" caused by the global pandemic and, as a consequence, they have had to review and even revise their contingency plans. It is very apt therefore that these expert authors have written a book that provides guidance and prompts on key considerations that are wholly appropriate to all sectors.'

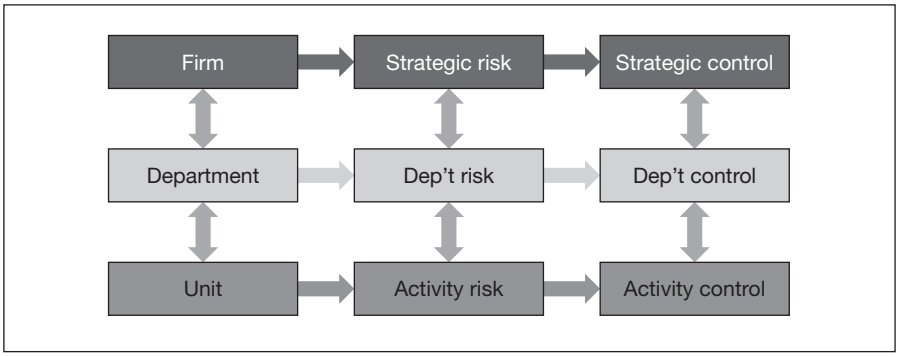
Marty Wright, Academic Head,
U2BInstitute, Glasgow Caledonian University

Figure 6.2 **Extract from a risk register with residual assessments and actions**

ID	Risks	Owner(s) of the Risk	II	IL	IS	RI	RL	RS	TI	TL	TS	Controls	Owner(s) of the Control	D	P	E	Action Plans / Comments
1	**Failure to attract, recruit and retain key staff**	SR	4	4	16	4	3	12	2	2	4	-Salary surveys	TJ	2	2	4	
												-Training and mentoring schemes	TB	3	2	6	
												-Retention packages for key staff	TJ	4	4	16	
2	**Financial advisors misinterpret / fail to understand the complexity of "equity release" products**	PL & AB	4	4	16	3	2	6	2	1	2	-Staff training	TB	4	4	16	
												-Learning gained from previous deals	KW & EL	4	4	16	
												-Review of individual needs in performance appraisal process	TB	3	2	6	
												-Procedure manuals for processes	EL	4	4	16	
3	**Poor staff communication**	SR & JK	4	4	16	4	3	12	2	3	6	-Defined communication channels	ZK	4	3	12	
												-Documented procedures and processes	EL	3	2	6	
4	**Failure to understand the law and/or regulations**	PL	4	3	12	4	2	8	4	1	4	-Internal training courses	EL	4	4	16	
												-Regular updates from various sources	EL	4	1	4	
												-External training courses	TB & EL	4	3	12	
5	**Poor detection of money laundering**	PL	4	3	12	4	2	8	3	1	3	-AML annual training	TB & EL	3	2	6	
												-Circulation of BBA awareness circulars	EL & ZK	3	1	3	
												-KYC	ALL	4	3	12	
6	**Insufficient funds/ deposits to cater for lending activities**	CK	4	3	12	4	1	4	3	1	3	-Liquidity risk policy	ZK	4	4	16	
												-Advertising	KW	4	3	12	
												-Economic forecasting	CK	3	3	9	
7	**Over-selling credit cards**	CK	4	3	12	4	1	4	2	1	2	-Staff training	TB	3	3	9	
												-Credit scoring	EL	4	4	16	
												-Forward business planning	ZK	3	3	9	
8	**Over-deployment of management resources on regulatory issues**	RU & CK	3	4	12	2	3	6	2	2	4	-Monthly budget against actual review	TJ	3	4	12	
												-Corporate governance	CK	4	4	16	
												-Monthly head of compliance & CEO meetings	CK	2	2	4	
9	**Failure to capture market opportunities**	AB	3	3	9	2	3	6	2	2	4	-Competitor monitoring	TB	3	4	12	
												-Product development	TB	2	2	4	
10	**Over-dependency on outsourcing**	OK	3	3	9	1	1	1	2	1	2	-SLAs	CK & EL	4	4	16	
												-Outsourcing monitoring	CK & EL	4	4	16	
												-Due diligence	CK	4	3	12	
												-Policy	CK	3	4	12	

Key: II Inherent Impact; IL Inherent Likelihood; IS Inherent Severity
RI Residual Impact; RL Residual Likelihood; RS Residual Severity
TI Target Impact; TL Target Likelihood; TS Target Severity
D Design; P Performance; E Effectiveness

Levels of risk and control self-assessment **Figure 6.3**



STRATEGIC RISK ASSESSMENTS (RISK ASSESSMENTS BY ANOTHER NAME!)

As noted above, strategic risk assessments identify the risks to the firm from meeting its business objectives. It is of course vital that the firm has identified these risks, or it will stand much less chance of surviving. It is surprising that many firms ignore strategic risk assessments and concentrate solely on risk assessments by department or process. While these are very useful, they are not focused on the strategic objectives of the firm.

Given the purpose of a strategic risk assessment, the risks identified are likely to be business-type risks such as the failure of an outsourcer or the loss of a member of the executive team. These will naturally have a more significant impact on the firm than the risks identified at a departmental level which are likely to be, for example, the failure of software used by the department or the loss of a supervisor within the department.

As well as wishing to achieve its strategic objectives, a firm should be looking to identify what it has to mitigate the risks that it has identified. These are the controls over the risks. The controls will also be assessed as well as identified and both of these are dealt with later in the chapter.

RISK IDENTIFICATION

Identifying risks (and their accompanying mitigating controls) should be a part of the firm's day-to-day business life and processes. Risk identification is a normal and natural part of being in business and should not be regarded as something that is done only once every six months or whenever a full risk assessment is performed.

Using the firm's objectives to identify risks

The use of a firm's objectives or goals to identify its strategic risks is the most natural place to start. The simple problem of "What will prevent me from meeting my objectives?" is one of the questions that the management asks itself many times during the year. By listing those things that will derail the objectives and assessing how good the firm is at managing the risks, senior management is simply performing one of the most important parts of its role. As well as using the firm's objectives, there are a number of other ways in which risks can be identified.

Using a risk library to identify risks

A risk library lists all the risks identified by a firm by risk. While it is useful to have a full list of risks identified by the firm, it can be constraining in a risk and control self-assessment, since participants tend to focus on the library rather than on what might prevent the firm from achieving its strategic objectives or goals. Given that one of the purposes of a risk and control self-assessment is to identify the risks, the existence of a risk library begs the question as to how the risks in the library were identified and to what the risks relate. If there is a risk library, put it to one side and start the risk and control self-assessment from scratch using the objectives or goals of the area being assessed. The library can be used later to validate the risks that have been identified and to check that no significant risks have been forgotten.

Using indicators to identify risks

Indicators show the movement in the likelihood or impact of a risk, in the design or performance of a control, or in the performance of a firm in relation to its objectives or processes. As such, existing indicators are useful in identifying the risks and controls on which the firm focuses. It is frequently possible to identify to which risk the indicators relate as the indicators are very often used to monitor the status of particular risks. However, key risk indicators (KRIs) and key control indicators (KCIs) are often mixed with key performance indicators (KPIs), so a first step is to sort the indicators (see Figure 7.2 and Chapter 7, Risk management and indicators, in general). Although there will be business benefit in sorting indicators into logical and consistent sets, this activity is likely to be outside the scope of a risk and control self-assessment and will therefore generally be undertaken separately.

Using audit findings to identify risks

Internal and external audit reports are also a good source of risks. However, auditors will often consider a control failure to be a risk. From a risk management perspective this is not true and a control failure should be thought of as simply that – a failure of a control. These lead to risks but are not risks themselves, i.e. a failure of a control is often the cause of a risk event occurring. For example, an ineffective salary review may lead to the loss of key staff. The risk is the loss of key staff – not an ineffective salary review.

Using losses to identify risks

Losses are the monetary result of a risk occurring. Losses are often collected by firms, particularly in reports to the risk committee or the audit committee. When loss causal analysis is used, this can be helpful in identifying the risks that have occurred and controls that have failed. However, the risks may have been identified without any reference to the business objectives or processes and are often couched as control failures, rather than as risks which resulted from the control failures. Again, care must be taken and additional work will probably be required for the analysis to be used in the risk and control self-assessment.

A firm's losses will only give a historical view of the risk to which it has previously been subject. It is therefore important to understand that there will be many more potential risks than are identified by a loss causal analysis.

See also Chapter 8, Risk management and events.

RISK ASSESSMENT

Once risks are identified, they are assessed for likelihood (sometimes called frequency) and impact (sometimes called severity). Likelihood is reviewed on the basis of how frequently a risk event will occur over a given period (e.g. monthly, three times a year, once in 5 years). Alternatively, many firms find it helpful to think of the percentage likelihood of a risk occurring in one year.

Impact is generally assessed on the basis of the (possible) cost to the firm if the risk happens. However, some risk occurrences such as reputation damage are difficult to assess on a cost basis. This more subjective impact is generally assessed on a qualitative scale such as high, medium high, medium, medium low and low.

While the term 'severity' is also used by some firms as being synonymous with impact, the word may also be used as a single value for a risk assessment, being a combination of likelihood and impact. This was more common before separate likelihood and impact assessments became widely used.

Assessment levels

Risks can be assessed at three levels of mitigation. Inherent (or gross) risk is assessed with no account taken of the controls which exist within a firm. The only controls which are assumed at the inherent level are inherent controls such as people's honesty and society's willingness to obey the law. The advantage of assessing risk at an inherent level is that there are no assumptions about the quality or existence (or otherwise) of controls. It also identifies the level of loss to which the firm is exposed if and when the existing controls fail.

Residual (or net) risk is assessed after allowing for the existing controls within the firm. This means that there are assumptions about the adequacy and continuing effectiveness of the controls. These assumptions are rarely stated in residual risk assessments. If they are stated, they become close to control assessments. The object of this part of the exercise is to assess risks, not controls. The level of loss arising from a residual risk assessment is the day-to-day loss which the firm may suffer with the existing level of control.

Target risk is the name often given to the final level of expected risk appetite which exists within a firm after all mitigating effects are at the firm's desired level. It is used to assess the impact (and sometimes the effectiveness) of control enhancement plans.

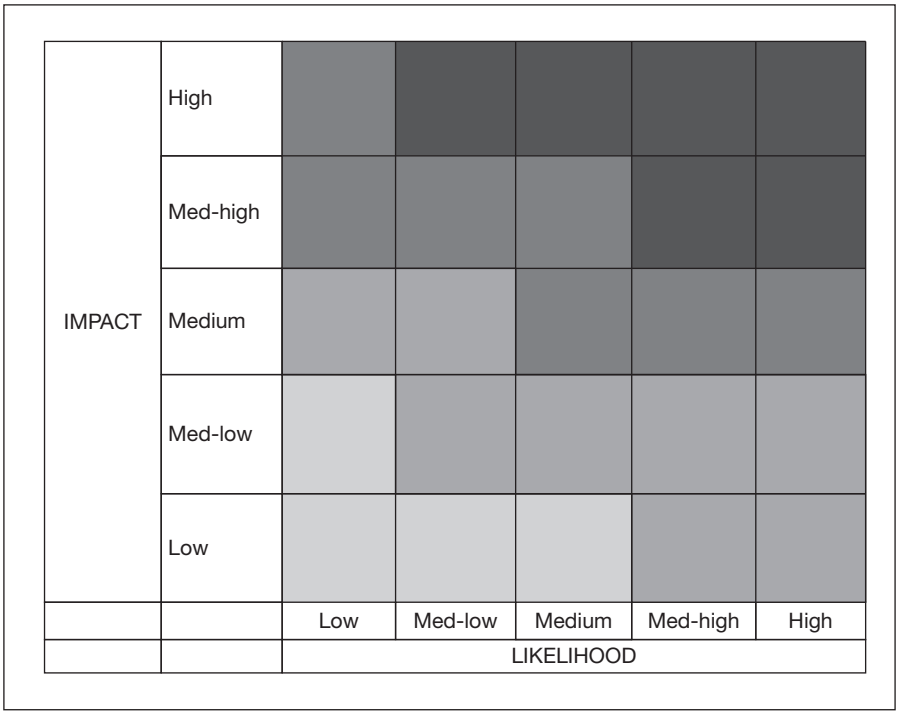
If risks are assessed at an inherent level, a control assessment can easily be linked to the inherent risk assessment. If risk is assessed at a residual level, the control assessment is already implicit in the residual risk assessment and the result will require reconciling back to an explicit control assessment.

Using heat maps to assess risks

Heat maps are a very common way to assess risks (see Figure 6.4). They generally use either four- or five-point scales, although five-point is becoming the standard as it gives more granularity than a four-point scale.

It is notable that the heat map in Figure 6.4 is not symmetrical. There are more dark squares (generally represented by red) in the top right-hand quadrant than there are light squares (generally represented by green) in the bottom left-hand quadrant as this firm considers impact more important than likelihood. It is also worth noting that the heat map in Figure 6.4 can be used for both inherent risk and residual risk. From an inherent risk perspective it is likely that a number of the risks will be in the dark squares (red) as no controls will be mitigating the risk. However, from a residual risk perspective there should be very few risks that are red, if any, as these risks will be very likely to happen if controls fail and will have a high impact as well. Any firm that carries that level of risk on a day-to-day basis will not last for very long.

Example of a five-point heat map **Figure 6.4**



When setting the impact scale points, many firms prefer to use gross revenues. This is useful because the business (the first line of defence) can directly influence it and therefore the use of gross revenues encourages embedding of the process. If net profitability is used, it must be borne in mind that it is more difficult for business heads to influence the costs allocated to them and they are therefore likely to be less willing to accept the scale. However, particularly in industries with a very low profit margin, gross revenues may be inappropriate and profitability may be more relevant.

The beginning point of the highest range is often set at three or four months of gross revenues or profitability, whichever is appropriate. The top end of the lower ranges can then easily be set at one month and one week if four ranges are being used. The full set of four being: above three months; three months to one month; one month to one week; below, one week. If five ranges are used, it is common to have an additional small range of two days, making the bottom two ranges one week to two days and below two days. You will notice that the top of each range is a multiple of around three to four of the one below. This is a useful rule of thumb when setting a scale.

The same approach is used for setting the scale for likelihood. The beginning point of the highest range for likelihood is often set at a level at which