RISK MANAGEMENT.

Checklist 266

» INTRODUCTION

Risk is part of life and all organisations face multiple risks, which may hinder or prevent them from achieving their objectives and can lead to operational disruption, escalating costs, loss of market share, reputational damage, financial losses or in the worst case scenario, business failure. But risks can also offer opportunities to embark on new business ventures, develop new products and services, increase market share and reap financial gains.

Risks may arise from internal factors relating to organisational processes, systems and people or come from external sources ranging from natural disasters and political upheavals to changes in the economy, the marketplace or the regulatory environment. Effective risk management gives organisations a better understanding of the kinds of risk they face and their potential impact. It enables managers to make informed decisions about how to eliminate or mitigate risk. It will also help them to be better prepared to respond to negative events, developing organisational resilience and sustainability. Ultimately, organisations which manage risk well will be more likely to achieve their objectives at lower overall costs.

Factors in the business environment such as the pace of change, increasing uncertainty and volatility, growing complexity and globalisation are highlighting the vital importance of risk management in the 21st century. High profile difficulties in the financial services sector during the first decade of the twenty-first century have also drawn attention to the shortcomings of traditional bureaucratic risk management practices and the need for a broader strategic approach to managing organisational risk. Our checklist on Strategic Risk Management covers this evolving approach (See Related checklists below). Nonetheless, at a time of increasing uncertainty, volatility and complexity in the economic and business environment, it is still vital for organisations to maintain efficient processes and procedures for monitoring and assessing factors which may have a negative impact on their operations, to be aware of the risks involved in new business ventures and to handle risk in an effective and proactive manner. This checklist aims to give managers a basic understanding of the principles of risk management and outlines a generic process for identifying and managing risk.

» DEFINITION

Risk has been simply defined as “the effect of uncertainty on objectives” (ISO 31000: 2009).

Risk management can be defined as the range of activities undertaken by an organisation to control and minimise threats to the continuing efficiency, profitability, and success of its operations. The process of risk management includes the identification and analysis of risks to which the organisation is exposed, the assessment of potential impacts on the business, decisions about appropriate responses to risk and the effective implementation of measures to avoid, minimise or manage the impacts of risk.

» ACTION CHECKLIST

1. Understand the organisational context

Risk management should not be divorced from organisational strategy. It needs to reflect organisational priorities and be integrated into decision making and resource allocation across the organisation. Before starting to identify and assess risks it is therefore important to be clear about your organisation's mission, vision and objectives. This will be particularly important when prioritising risks and deciding how best to handle them.

Senior managers and the board carry responsibility for the overall organisational framework for managing risk and must be seen to be committed to it. An organisation's ability to weather storms depends on how seriously senior executives take risk management. Senior managers should also take responsibility for defining acceptable levels of risk – the organisation's 'risk appetite' – and ensuring that this is communicated and acted on. If risk appetite is too high the organisation will be put at risk; if it is too low the organisation may miss out on profitable opportunities.

2. Distinguish between different types of risk

Risks can be categorised in a number of different ways. They may be the result of internal factors such as failure to follow health and safety procedures, employee theft or fraud; or they may come from external sources, such as natural disasters, economic instability or changes in government policies and legislation. They may be relatively predictable or they may be completely unexpected, such as the 'black swan' events identified by Nassim Nicholas Taleb. They may be preventable - inefficient processes, for example, or unavoidable as in the case of natural disasters. They may be wholly negative in their impact or, as with the risks inherent in the development of a new product, they may carry the potential for financial rewards and increased market share. Different types of risk will need to be handled in different ways.

When assessing organisational vulnerabilities, it is important to be aware that the risks to which an organisation is exposed will depend on its size, the nature of its activities and the sector in which it operates. Companies in the pharmaceutical industry, for example, face risks related to the handling of hazardous substances which will be irrelevant to many service sector organisations.

3. Identify risks and potential causes

Every aspect of an organisation's operations involves risk, so it is important to take a broad overview. Key areas to focus on include:

- physical assets – buildings, equipment, machinery
- workplace health and safety - working conditions, hazards, including dangerous substances
- IT and telecommunications systems - robustness, security
- intellectual property – including patents and trademarks
- people issues – allegations of discrimination, loss of key people, inadequate training, difficulty in recruiting employees with the right skills and knowledge
- supply chain issues – problems with suppliers, transport disruptions, customer complaints
- financial risks – cash flow and liquidity, currency fluctuations, poor returns on investment
- regulatory compliance –failure to comply with legislative requirements. Additionally, legislative changes may affect how the organisation does business
- strategic risks – due to changes in the marketplace or the business environment.

A range of methods can be used to gather information including:

- brainstorming sessions
- interviews
- questionnaires
- the Delphi technique
- checklists
- consultation workshops

- incident investigation
- inspection
- auditing and review.

Identified risks, their causes and potential impacts should be listed and described in an organisational risk register. Our checklist on conducting a project risk assessment includes more detail on risk registers (See Related checklists below.) Don't forget that risks are inter-related and that a risk in one area of the business may have knock-on effects on other parts of the organisation.

4. Analyse and evaluate risks

It is vital to ensure consistency by introducing standard criteria for assessing risks. For each risk identified two main factors should be considered: probability and impact. The criteria should define what level of likelihood would be considered to be: almost certain, moderate or unlikely, for example, and what level of impact would be considered minor, major or catastrophic. Once criteria have been set, a risk map or matrix can be used to rank risks as low, medium or high. This will enable you to prioritise those risks that will have the most serious effects on the organisation. Additional factors to consider are potential costs and time scales – is the risk likely to have an impact in the short-, medium or long-term?

A range of techniques may be used to analyse risk including:

- Failure Modes and Effects Analysis (FMEA)
- Scenario analysis
- Monte Carlo method
- Business impact analysis (BIA)
- COBRA (Consultative, Objective and Bi-functional Risk Analysis) - used to assess IT security

The results of the analysis should be added to the risk register, showing the cause, potential impact, likelihood and ranking of all identified risks.

5. Decide how to respond to risk

One commonly used approach to developing responses to identified risks is known as the 4 Ts of risk management:

- Tolerate - where a risk is insignificant and/or unavoidable but offers potential opportunities for profitable growth, managers may decide to tolerate it
- Treat - in the case of a clear internally generated risk, measures to treat the risk would be more appropriate. Risk treatment options might involve mitigating the risk by introducing control measures or reducing the impact by developing business continuity, contingency management or disaster recovery plans.
- Transfer - in some cases risk can be transferred by outsourcing a function to a specialist external provider with better back-up and specialist skills or shared by taking out insurance policies or amending the terms of contracts.
- Terminate - in some cases, it may be deemed wise to terminate risk. This might involve removing the source of the risk, if feasible, or stopping an activity altogether, by, for example, exiting a market where the risks have begun to outweigh the anticipated gains.

Organisational responses to risk need to be proportionate to the level of risk and appropriate to the nature of the risk. As mentioned in point 1 above, decisions on whether to tolerate, treat, transfer or terminate risks should be in line with the organisation's stated risk appetite.

6. Take appropriate action to mitigate or eliminate risk

Once risks have been identified and prioritised, detailed plans of proposed responses can be developed, and again this should be recorded in the risk register. As well as details of proposed actions, plans should cover details of the people accountable for implementation and the resources needed, as well as time scales, and performance measures. In larger organisations this may involve the development of an integrated enterprise risk management (ERM), but all organisations need to consider the extent to which risk management needs to be integrated across the business.

7. Ensure compliance with regulatory requirements

Although, risk management is not limited to compliance with legislative requirements, it is important to identify legislation with which the organisation must comply, to put appropriate systems and procedures in place, and to ensure that all relevant personnel are aware of the requirements. Responsibility for monitoring changes in the regulatory environments which will affect the organisation should be allocated to a suitable person or team, so the need for change can be flagged up and acted on whenever necessary.

8. Encourage a culture of personal responsibility

It is important that responsibility for risk management is not seen solely as the responsibility of a single department or function within the organisation. Dedicated risk management departments have a role to play in overseeing risk management systems and processes, especially in larger organisations, but it is also vital to promote positive risk management attitudes and behaviours and develop a culture of risk awareness right across the organisation. Individuals need to be encouraged to take responsibility for risk management at their own level. It has been found that managers tend to under-estimate risks and be over-confident about the accuracy of forecasts, especially where there is a history of success. Groupthink can also mean that significant risks are overlooked and doubtful suppositions go unchallenged. Clear communication and a 'no-blame' culture will be important here. Consider also, building incentives into performance management and reward systems so that individuals feel free to raise any issues and concerns.

9. Monitor, review and report

Effective risk management is a continuous, ongoing process, not a one-off exercise. Keep in mind that the levels and types of risk to which an organisation is exposed are subject to continual change both internally and externally. Procedures need to be in place to monitor the evolving operations of the organisation and developments in its operating environment.

It is essential to put procedures in place for monitoring risk management practices, assessing their effectiveness, ensuring that they are being correctly implemented and making any improvement and amendments that become necessary. Methods used to gather information may include inspections, incident investigations, audits and formal reviews, questionnaires and interviews, or consultations and discussion.

Good risk reporting will help to ensure accountability and inform decision making in the future. Reports should be timely, tailored to the audience, focus on key messages and be presented in an accessible format.
Text.

» POTENTIAL PITFALLS

Managers should avoid:

- focusing on a narrow range of risks
- forgetting to keep the risk register up to date
- seeing all risk as negative

» ADDITIONAL RESOURCES

BOOKS

Fundamentals of enterprise risk management: how top companies assess risk, manage exposure, and seize opportunity, 2nd ed., John J Hampton
New York NY: AMACOM, 2015

The risk doctor's cures for common risk ailments, David Hillson
London: Berrett-Koehler, 2014

Risk management, Paul Hopkin
London: Kogan Page, 2013

Winning with risk management, Russell Walker
Singapore: World Scientific, 2013

A short guide to facilitating risk management: engaging people to identify, own and manage risk, Penny Pullan and Ruth Murray-Webster
Farnham: Gower, 2012

A short guide to operational risk, David Tattam
Farnham: Gower, 2011

Fundamentals of risk management: understanding, evaluating and implementing effective risk management, Paul Hopkin
London: Kogan Page, 2010

JOURNAL ARTICLES

Risks and quality: an Australian case, Matthew Mackenzie and David Parker
Management Services, Summer vol 58 no 2, 2014, pp20-24, 36

Managing change and building a positive risk culture, Philip Atkinson
Management Services, Summer, vol 57 no 2, 201

Risk management: the next source of competitive advantage, Ehsan Elahi
Foresight, vol 15 no 2, 2013, pp117-131

Managing risk: a new framework, Robert S Kaplan and Anette Mikes
Harvard Business Review, June vol 90 no 6, 2012, pp48-58, 60

RELATED CHECKLISTS

050 Spotting fraud
056 Health and safety: undertaking a risk assessment
241 Conducting a project risk assessment
255 Business continuity planning for major disruptions
264 Strategic risk management

INTERNET RESOURCES

Health and Safety Executive Risk
http://www.hse.gov.uk/risk/index.htm
Provides general guidance on risk management intended primarily for small companies and offers interactive tools, example risk assessments and templates**.**

ORGANISATIONS

The Institute of Risk Management, 6 Lloyd's Avenue, London EC3N 3AX
Tel: 020 7709 9808 Web: www.theirm.org

Health and Safety Executive, Redgrave Court, Merton Road, Bootle, Merseyside L20 7HS
Tel: 0300 003 1747(Advisory Team) Web: www.hse.gov.uk

Airmic, 6 Lloyd's Avenue, London EC3N 3AX
Tel: 020 7680 3088 Web: www.airmic.com

» CMI PROFESSIONAL STANDARDS

This checklist has relevance for the following standards:

- OP2.4 Managing risk
- OP2.5 Ensuring compliance

» MORE INFORMATION

e enquiries@managers.org.uk **t** +44 (01536) 204222 **w** www.managers.org.uk

p Chartered Management Institute
Management House, Cottingham Rd, Corby, Northants, NN17 1TT

Revised February 2020