

BS 31100:2008 Risk management. Code of practice (sample pages)

Contents

Foreword	<i>ii</i>	
Introduction	<i>1</i>	
1 Scope	3	
2 Risk management principles		3
3 Risk management framework		5
4 Risk management process		16
5 Developing risk management activities	22	
Annexes		
Annex A (informative) risk categories	26	
Annex B (informative) risk management tools	27	
Annex C (informative) Effects of controls	29	
Annex D (informative) risk maturity models	31	
Annex E (normative) incorporating potentially positive consequences of risk	32	
Glossary	33	
Bibliography	40	
List of figures		
Figure 1 – risk management perspectives	2	
Figure 2 – risk management model	2	
Figure 3 – risk management framework	5	
Figure 4 – the risk management process	16	
List of tables		
Table B.1 – Examples of risk management tools (including techniques)	28	

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 31 October 2008. It was prepared by Technical Committee RM/1, *Risk Management*. A list of organizations represented on this committee can be obtained on request to its secretary.

This British Standard has been developed by practitioners throughout the risk management community, drawing upon their considerable academic, technical and practical experiences of risk management.

Relationship with other documents

This British Standard has been drafted to be consistent with the general guidance on risk management that will be given by ISO 31000 (in preparation), but is also developed recognizing the knowledge contained in HM Treasury's Orange Book [1], the Office of Government Commerce publication, "*Management of risk: Guidance for practitioners*" [2], "*Enterprise Risk Management — Integrated Framework*" and application techniques published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [3], and the risk Management Standard developed by the Institute of Risk Management (IRM), the association of insurance and risk Managers (AIRMIC) and ALARM [4].

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The word "should" is used to express the recommendations of this standard, with which the user has to comply in order to comply with the standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Organizations of all types and sizes face a range of risks affecting the achievement of their objectives. While “risk” is commonly regarded as negative, risk management is as much about exploiting potential opportunities as preventing potential problems. It is important to bear this in mind whenever managing risk, and in reading this Code of Practice. Risk management is an essential part of good management.

Effective risk management can assist the organization to achieve its objectives by, for example:

- a) reducing the likelihood of events that would have a negative consequence overall and reducing the negative consequences of such events;
- b) increasing the likelihood of events that would have a positive consequence overall and increasing the positive consequences of such events;
- c) identifying opportunities where taking risks might benefit the organization;
- d) improving accountability, decision making, transparency and visibility;
- e) identifying, understanding and managing multiple and cross-organization risks;
- f) executing change more effectively and efficiently and improving project management;
- g) providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements;
- h) protecting revenue and enhancing value for money;
- i) protecting reputation and stakeholder confidence;
- j) proactively managing the organization’s operations;
- k) targeting control expenditure and delivering a cost-optimal control environment;
- l) retaining and developing customers through reducing risks to service delivery and enhancing service provision; and
- m) making the organization more flexible and responsive to market fluctuations so that it is better able to satisfy customers’ ever-changing needs in a continually evolving business environment.

The benefits of good risk management (and the consequences of poor risk management) will be felt by an organization’s management, staff, shareholders, customers and other stakeholders.

Risk management has to continuously, systematically and proportionally address the risks surrounding an organization’s activities. It cannot be separated from the culture of the organization.

Risk management comprises a framework and process that enable an organization to manage uncertainty in a systemic, effective, efficient and systematic way from strategic, programme, project and operational perspectives, as well as supporting continual improvement.

Risk management applies at all levels of an organization and to all activities (see Figure 1 [not included in sample pages]).

This standard provides a guide to risk management principles, models, framework and processes. Its purpose is to assist organizations to achieve their objectives through effective risk management.

The risk management model presented in this standard provides at the core a framework and process on which to manage risks. The outer rings of Figure 2 [not included in sample pages] contain the context in which the organization operates, the organization itself and the culture, with communication required at all levels.