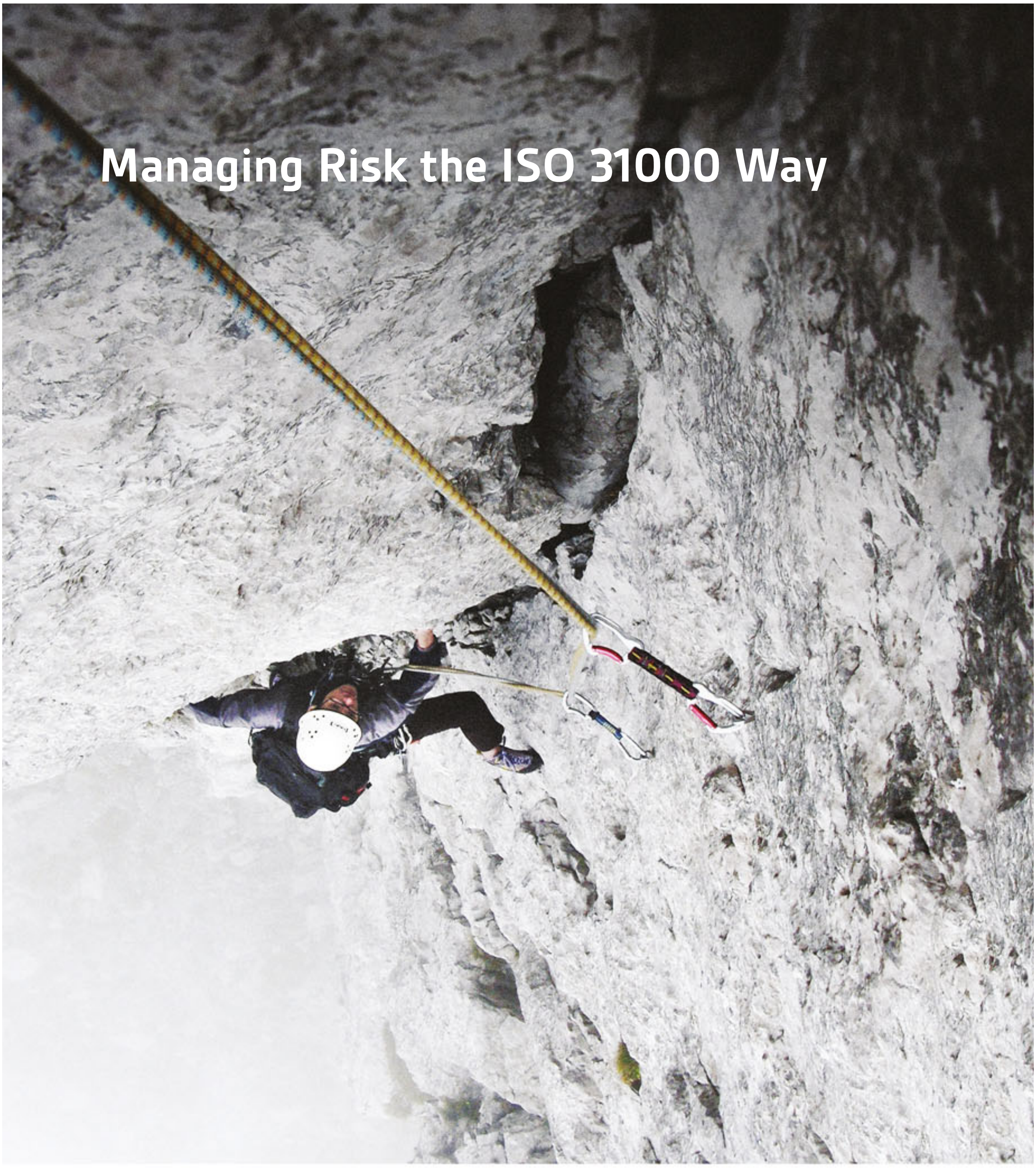
Managing Risk the ISO 31000 Way



David Smith and Rob Politowski

Managing Risk the ISO 31000 Way

Managing Risk the ISO 31000 Way

By David Smith and Rob Politowski

bsi.

First published in the UK in 2013

By
BSI Standards Limited
389 Chiswick High Road
London W4 4AL

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

While every effort has been made to trace all copyright holders, anyone claiming copyright should get in touch with the BSI at the above address.

BSI has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Typeset in Great Britain by Letterpart Limited

Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978-0-580-67512-6

Contents

Acknowledgements

The authors would like to thank the book reviewers and particularly Michael Faber for his constructive comments. The authors would also like to thank GPIC Bahrain and RTA Dubai for allowing them to see the good practices that they have implemented in line with ISO 31000.

Chapter 1 - Introduction

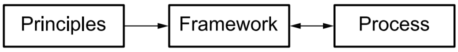
All organizations face many risks, some of which will be well known and managed. Others may pose significant threats to the organization and may well be ignored or poorly managed. It has to be recognized that it is unlikely all risks will be identified, but the aim for all organizations should be to create a framework that:

- manages risks that are identified;
- provides a structure for dealing with risks that emerge which have not been identified; and
- creates a more resilient organization, enabling it to respond to future risks in a time of need.

The whole question of risk has now attracted the attention of the media around the world and examples of poor risk management and governance regularly hit the headlines. The consequences of poor risk management are all too evident in how they can affect us all, as taxpayers, workers and consumers, as well as in the impacts they can have upon the environment and society in general.

Risk and its effective management is the subject of significant numbers of publications and academic work. Whilst these approaches have much merit they are often perceived to be far too complex for the smaller organization and it is the small- to medium-sized businesses at which this book is primarily aimed, i.e. smaller organizations seeking simple guidance on the implementation of an effective risk management system that brings real benefits. This book is intended to help organizations survive and thrive in an ever changing world, a world where those organizations that do not embrace risk management may fail.

The ISO 31000 standard for managing risk has three main components:



The standard identifies 11 core principles of risk management with the intention that these will be addressed by the development of the risk management framework. In turn, the framework assists in managing risk through risk management processes.

In large, complex organizations there may be many hundreds, or even thousands, of risks, many of which will not be significant or will have well-established controls in place, such as emergency evacuation plans. Smaller organizations that are not complex may have fewer significant risks. The framework proposed in ISO 31000 indicates that management of individual processes are typically separate arrangements.

In many organizations there are well-established, formal systems to manage specific risks that are based on international standards such as quality (ISO 9001), environment (ISO 14001), information security (ISO/IEC 27001), food safety (ISO 22000), business continuity (ISO 22301) and occupational health and safety (OHSAS 18001), which have been accommodated within the overall management system of the organization. In some cases, this is a regulatory requirement. The management system in operation, particularly if it is based on an integrated approach such as that prescribed in PAS 99, may well be seen as a foundation for the framework. This book provides guidance in developing a mechanism for managing risk in accordance with ISO 31000, where necessary including the good practices outlined in BS 31100 and PAS 99 for managing processes in an integrated manner.

Whilst the two risk management publications, ISO 31000 and BS 31100, provide an excellent framework, there are a number of areas in both standards where there is no substantive guidance. In these areas, such as policy statements, internal auditing and management reviews, this book provides considerable extra guidance with examples, where appropriate. In those areas where the additional guidance provided by BS 31100 in support of ISO 31000 is good, this information has been used as the basis for the guidance in this book, supplemented with additional material and examples, where appropriate.

The book is based on the international standard ISO 31000 and utilizes support documents such as PAS 99 and IEC/ISO 31010.

In this chapter the following items are covered:

- What is risk management?
- Why should an organization bother with risk management?
- Which organizations should implement risk management systems?
- What are the principles of a risk management system?
- How should this book be used?

What is risk management?

There are many definitions that are used in the area of risk management and, as the reader works through the book and new terms are introduced, the definition and a full explanation is provided where it is felt this is necessary for understanding. Readers may find it useful to consult other specific definitions in ISO 31000, BS 31100 and ISO Guide 73 if they need further clarification.

For those who are starting on the journey, there is a need to put risk and risk management into context. Risk is defined as the:

> effect of uncertainty on objectives
>
> ISO Guide 73, Clause 1.1

This definition may not mean much to those with little experience in the area of risk management. In order to give some more clarity, ISO 31000 provides the following guidance by way of notes to the main definition (see also Figure 1):

> **risk**
> effect of uncertainty on objectives
>
> NOTE 1 An effect is a deviation from the expected — positive and/or negative.
>
> NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
>
> NOTE 3 Risk is often characterized by reference to potential events…and consequences…, or a combination of these.
>
> NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood…of occurrence.
>
> NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Organizations need to plan to achieve their objectives and, in doing so, have to evaluate the benefits of achieving the objectives and determine what might prevent them succeeding. Logistics issues, lack of parts from a supplier, failure of equipment, poor service by the sales department, etc. can all be issues that may be important in the ability to deliver objectives. Decisions can then be made on whether the risk is worth taking because of the potential benefits and, if so, what treatment or controls should be applied to minimize the risk of not succeeding.

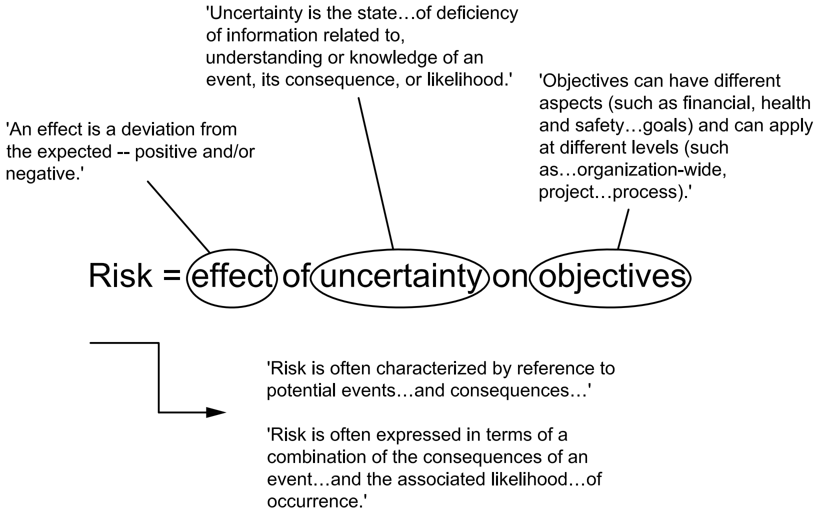

'Uncertainty is the state…of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.'
'Objectives can have different aspects (such as financial, health and safety…goals) and can apply at different levels (such as…organization-wide, project…process).'
'An effect is a deviation from the expected -- positive and/or negative.'
Risk = effect of uncertainty on objectives
'Risk is often characterized by reference to potential events…and consequences…'
'Risk is often expressed in terms of a combination of the consequences of an event…and the associated likelihood…of occurrence.'

Figure 1 — Definition of risk

ISO 31000 and ISO Guide 73

Risk can be considered as the combination of the likelihood of an event happening and the consequences of that event. At a personal level we all take risks. For example, we may wish to cross a main road to obtain items that can only be conveniently obtained from a shop across the road. The decision to cross a road is an obvious risk. The road is very busy and the risk could be as severe as injury, or even death, if we are involved in an accident.

Various options are available:

- not to bother because the risk is too great (*risk aversion)*;
- ask someone else to undertake the task for us (*risk transfer*);
- cross the road, taking the risk ourselves, having made an assessment (albeit subconsciously) of the situation.

Once the decision has been made to cross the road, accepting the risk, most people would make provision to minimize the risk of harm. The risk could be ‘managed’ by various means including:

- the use of a pedestrian crossing;
- crossing at a place where traffic is light and there is good visibility.

This simplistic case is given as a case of 'risk management':

> 'co-ordinated activities to direct and control an organization with regard to risk'
>
> ISO Guide 73, Clause 2.1

We identify a risk (the degree of harm in this case and the likelihood) and take steps to manage the risk. We all face a number of differing risks every day and seek to manage these in different ways, e.g. when purchasing a house we take on a financial risk and may decide to insure against loss caused by flooding, a storm, fire, etc.

Why should an organization bother with risk management?

Organizations take risks, whether they are public service bodies, large companies or charities. In taking these risks, they learn more about their activities, enabling them to become more successful in the future. Take, for example, the first heart transplant operation. If the risk had not been incurred and subsequently managed, learning from this process, this procedure would not be the relatively common and comparatively safe operation that is routinely performed today. Businesses have to take a risk when they develop a new product – hoping that their research and development (risk management) was sufficient to generate a return on the investment. Charities can take a risk when they decide to intervene with aid because the aid may not get to the targeted beneficiaries and may be used by exploitive parties for their own benefit.

Examples of the impact of poor risk management upon both organizations and society:

- lending in the subprime mortgage market in the USA;
- rogue traders in the investment banking sector;
- poor management of food hygiene leading to closure of food outlet;
- failure to maintain public service vehicles adequately, leading to withdrawal of operating licence;
- oil leak in Gulf of Mexico in 2010.

Given the myriad of risks that an organization can face, it is clear that there is substantial benefit to be obtained by taking on a more formal risk management approach in order to avoid:

- damage to its reputation;
- loss of its customers through failure to provide a service or product (in the public sector it may mean the loss of patients using a hospital facility);
- damage to financial viability through loss of share value, loss of access to capital, etc.;
- difficulties with interested parties, e.g. neighbours, regulators, customers and workforce.

Whilst the above are some basic reasons why an organization should bother with managing risks, it is not an exhaustive list. Some risks are positive but many see risks as being a negative threat to the organization. In reality, risks need to be managed to positive effect where possible. The approach given in this book should be equally useful to those who deliberately take risks in the hope it will provide positive benefits to the organization.

Risk management is not just something that is important to the financial sector. Poor risk management has led to many catastrophic outcomes and, equally, a positive attitude to risk taking has resulted in many of the great achievements we witness on a daily basis. The primary purpose for organizations to implement and operate effective risk management systems is to survive and thrive.

Effective risk management systems should enable an organization to achieve its objectives by, for example:

- reducing the likelihood of an event that could have an adverse effect on the organization’s ability to deliver its product or service, or reducing the consequence should such a situation arise. For example, if a company relies on a particular logistics supplier and there is a risk that it may fail in some way, provision should be made for an alternative arrangement with an in-house backup or an alternative logistics company;
- increasing the likelihood of success by putting effective measures in place, e.g. additional sales support staff when opening a new shop to ensure shoppers get a good experience and feel that there is plenty of help for them when making purchases;
- ensuring that the organization identifies opportunities where taking risks might benefit the organization, e.g. staff suggestion schemes;
- improving accountability, decision making, transparency and visibility in order to ensure that personnel understand their role and the outcome of not managing the risk they impact upon;
- identifying, understanding and managing multiple and cross-organization risks, as it is common to find that each risk cannot necessarily be isolated into one ‘box’ and may impact on other parties. The introduction of a water-based paint product into a bodywork shop may be advantageous from health and safety and

environmental aspects, but if it slows down production and prevents working on the panels for, say, 24 hours versus 2 hours there could be a number of adverse impacts;

- executing change more effectively and efficiently and improving project management. It is quite common to find that changes can be implemented in the organization, system, etc. without first evaluating the overall impact prior to implementation. The management of change is an essential element to ensure effective and efficient changes;
- providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements;
- protecting revenue and enhancing value for money. It is sometimes better to put in place robust measures that protect the revenue, as well as devote resources to marketing and sales. A high turnover in customers is something to avoid, where possible, and it is better to keep existing customers happy as well as seeking new ones. The effort expended in gaining new customers will often greatly exceed what is needed to keep existing customers;
- protecting reputation and stakeholder confidence. Organizations depend on having a good reputation and on their stakeholders, such as customers, insurers, neighbours, workers and suppliers, having confidence in them.
- differentiating you against your competition: demonstrating good risk management can be an enabler to winning business.

Which organizations should implement risk management systems?

Risk management is a universal issue that is common to governments, public bodies, corporations, institutions and charities, regardless of their size or sector.

What are the principles of a risk management system?

One of the first steps when setting up a framework for managing risk is to determine the principles that should be followed. Guidance is provided on this subject in Chapter 3 to support the principles given in ISO 31000, and links are given to show how the implementation of risk management should deliver these principles.

How should this book be used?

This book is primarily written for those organizations that do not necessarily have a formal organization-wide risk management system. It is recognized that many will have systems for managing occupational health and safety because it is a legal requirement; others will have systems for quality (ISO 9001), environmental management (ISO 14001), information security (ISO/IEC 27001), food safety (ISO 22000), business continuity management (ISO 22301) or social accountability (SA 8000), etc. The frameworks for managing these areas of risk may well be the foundation for the risk management system and it would be both costly and time-consuming to build a totally new system, which could be burdensome and could cause duplication, confusion and unnecessary bureaucracy.

Those organizations that do not have any formal system in place may also find the approach put forward in Chapter 12 helpful, as it will simplify implementation of other management systems at a later stage.

Whilst ISO 31000 provides a foundation, this book offers a full and considered approach that can be applied by those wanting to expand their existing management system to an enterprise-wide risk management system, as well as by those looking at risk management in isolation. To help those readers who are new to this subject a simple case study is used from time to time to give some appreciation of what is involved.

Chapter 2 - Getting started

The following chapters provide a structured approach to implementing a risk management framework and associated processes into an organization. Based upon ISO 31000 and BS 31100, together with supporting guidance, it will help the reader in the implementation and operation of a formalized risk management system. The overlap and repetition found in the standards has been eliminated, where possible, in order to simplify the process whilst retaining important points.

All organizations will have some arrangement in place for managing individual risks, although they may not necessarily realize it, have the formal framework or have any processes in place. The scope of the task for developing and implementing a risk management framework and managing risk is set by the context of the organization. By context we mean the ‘world’ in which it operates, who it serves, the expectations of its customers and/or shareholders, etc.

The matrix in Table 1 provides the links between the book chapters and the clauses in ISO 31000 and BS 31100, which are aligned in most cases. Subjects such as ‘Understanding of the organization and its context’ (Clause 4.3.1) and ‘Establishing the context’ (Clauses 5.3.1, 5.3.2, 5.3.3 and 5.3.4) are covered in Chapter 5, rather than in separate chapters. An additional column is provided for indicating whether the issue has been addressed at your organization.

Table 1 — Initial status review correspondence

Chapter heading	Corresponding clause(s)	Addressed: Yes/No
1 Introduction		
2 Getting started		
3 Principles	3	
4 Leadership, commitment and culture	4.2	
5 Context	4.3.1; 5.3.1; 5.3.2; 5.3.3; 5.3.4	
6 Framework	4	
7 Risk management and implementation	4.4, 5.4	
8 Risk treatment and implementation	5.5	
9 Monitoring and review	4.5; 4.6	
10 Internal auditing	4.5	
11 Recording and reporting	4.3.6; 4.3.7	
12 Integrating your management systems	4.3.4	

Those organizations with established management systems may find a benefit in reading Chapter 5 and Chapter 12 before deciding how to proceed with the development and implementation of a risk management system.

To help smaller organizations, or those new to the subject area, understand how to implement risk management, a hypothetical organization is provided to illustrate some of the key challenges and considerations raised in the following chapters. The journey towards a system for managing risk is picked up at relevant points. The example is not intended to be perfect and the approach taken by the fictitious characters is not necessarily sound all the way through, as this would defeat the objective. The idea is to show what might happen and the thought processes involved along the way.

Case study – Gillie's T 4 2

'Gillie's T 4 2' is a small tea shop and café in a village called Aston-by-Water. It is very successful and is well patronized by the locals, as well as visitors who come to the area for tourism. Gillie is very happy with her success, built up since establishing the business seven years ago. Having said this, she had never thought she would be so successful that she would take the neighbouring shop over and employ 30 employees to cover the various hours the shop and café are open.

One day, a regular customer at her café said: 'May I have a word with you sometime?' She was alarmed in case something was wrong but he quickly reassured her with a charming smile and said: 'I would like to talk to you about us jointly growing your business so you can become a household name.'

As it turned out, Rob, the customer, had been successfully selling second-hand cars and had retired. He now wished to invest. He had built his own business on maintaining high standards and had found that the principles in ISO 9001 had helped him a lot. He had recently read about a new standard for managing risks, which he had found thought-provoking. He said to Gillie: 'Don't worry about how we'll develop your business. I will sort out your "external context" if you can deal with the "internal context" to start with.' Gillie was confused and so Rob went through the ISO 31000 process with her; she needed two pots of coffee to stay awake. Thankfully, Gillie was aware of ISO 9001 for quality management and so was not too fazed by the risk management process that Rob explained so enthusiastically. He had been reading the standard and getting to grips with its implications, and wanted to try it out in practice with a new investment.

Immediately, Gillie wondered how an expansion of her business would affect the relationships with the café's suppliers that were so integral to the success she enjoyed. Her friend, Jane Lovecake, ran the nearby bakery. It was her bread, pastries and cakes that she had used for many years and knew to be as big an attraction for her customers as her tea and service. Gillie grew concerned that if she rapidly expanded her business she would not be able to rely upon the small, local network of businesses to meet the increased demands.

Gillie's journey towards a system for risk management for her business is picked up again in the following chapters.