# Risk Management Guidelines

*Expert knowledge means success*

Contents


1. Introduction
1. What is Risk Management?
2. Basic Risk Controls
4. How Do You Score?
5. Recommended Reading
5. Risk Management Standard
6. Further Information

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

# Introduction

All businesses need to have controls in place to ensure that they are able to function efficiently and effectively and reduce their vulnerability to fraud, malicious intrusion and other forms of unauthorised activity or interference. This publication looks at some of the areas involved and offers outline guidance for business controls in connection with the prevention of financial losses. In particular, we draw to your attention the Risk Analysis programme – an in-depth review of most areas of the activities of a business with guidelines for action based on the outcome of the report it generates.

Understanding business risks and risk management should be a primary concern of all businesses, regardless of the size. In essence, business protection, insurance and risk management go hand-in-hand. Risk management is as much about the identification of opportunities as avoiding or mitigating losses.

While it is not possible to prevent all hazards, the objective of risk management is to:

- reduce risks to an acceptable level;
- reject unacceptable risks; and
- transfer other risks through insurance and other means.

A proven track record in controlling risks may also result in reduced insurance premiums over time and contribute to the long-term success of your business.

# What is Risk Management?

Risk management is a methodical process used by a business to determine and address the risks associated with its activities with the objective of increasing the probability of success and decreasing the probability of failure. It is a discipline that aims to protect assets and profits by reducing the potential for loss before it occurs, and by financing, through insurance and other means, potential risks to catastrophic loss.

As mentioned above, whilst it isn't possible to prevent all risks, the aim should be to minimise or reduce the risk, or the effects of the risk. The initial damage following a loss or accident can be just the tip of the iceberg. Research shows that uninsured losses can often be significantly greater than the amount covered under the insurance policy.

These "hidden costs" are often not considered and can include:

- Waste of time and increases in business costs;
- Customers switching to other suppliers;
- Missed new business opportunities (while business is not operating);
- Consequences of the delay in returning to full operations (losing staff to competitors etc.);
- Cancelled orders may affect business relationships;
- Damage to reputation and brand.

With this in mind, it makes good business sense for a company to implement a risk management program in order to minimise the risks to the business.

## Risk Management Standard

The objectives of risk management can be achieved through a number of different approaches and processed. There are however risk management standards available should a company wish to measure their implementation of risk management against a standard.

The Institute of Risk Management publishes a risk management standard in conjunction with ALARM - The National Forum for Risk Management in the Public Sector and AIRMIC - The Association of Insurance and Risk Managers. More information is available at the end of this publication and at: www.theirm.org

The International Standards Organization publishes the terminology used in Risk Management in its publication ISO/IEC Guide 73 Risk Management – Vocabulary – Guidelines for use in standards. More information is available at: www.iso.org.

## Functions of Risk Management

The Carnegie Mellon Software Engineering Institute (www.sei.cmu.edu) says that each risk goes through the functions (shown below) sequentially, but the activity occurs continuously, concurrently (e.g., risks are tracked in parallel while new risks are

### Risk Management – an integral part of business practice

"Risk management is recognised as an integral part of good management practice.

To be most effective, risk management should become part of an organisation's culture. It should be integrated into the organisation's philosophy, practices and business plans rather than be viewed or practiced as a separate program. When this is achieved, risk management becomes the business of everyone in the organisation.

Risk management is the term applied to a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk associated with any activity, function or process in a way that will enable organisations to minimise losses and maximise opportunities. Risk management is as much about identifying opportunities as avoiding or mitigating losses."

*Source: InterDynamics* www.interdynamics.com.au

### What is risk?

Risk is the combination of the probability of an event and its consequences.

*Source: ISO/IEC Guide 73*

identified and analysed), and iteratively (e.g., the mitigation plan for one risk may yield another risk) throughout the project life cycle.

| Function | Description |
|---|---|
| Identify | Search for and locate risks before they become problems. |
| Analyse | Transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritise risks. |
| Plan | Translate risk information into decisions and mitigating actions (both present and future) and implement those actions. |
| Track | Monitor risk indicators and mitigation actions. |
| Control | Correct for deviations from the risk mitigation plans. |
| Communicate | Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks.<br>*Note*: Communication happens throughout all the functions of risk management. |

# Basic Risk Controls

Acknowledgement: This section is based on a paper issued by Royal & Sun Alliance. These points are of a general nature, and do not take into account individual circumstances. You should always consider consulting a professional adviser to help tailor your plans to suit your own business environment.

## Overview

The level and range of controls needed will vary significantly according to the nature and size of the business, but every business should at the very least do the following:

- Ensure that management fully understand the business they manage or run
- Ensure that all business activities are identified and nominated individuals accept responsibility for managing them
- Carry out assessments of risk throughout the business and prioritise and implement action needed to manage them
- Ensure that there is a clear segregation of duties so that for example no single individual can move or purchase or use or order or sell assets without the express approval and knowledge of another authorised person
- Monitor and audit the effectiveness and implementation of business controls and identify and implement changes needed.

For Stock Exchange listed companies the need for high standards of corporate governance is summarised in the Combined Code on Corporate Governance and must be followed. This code was further enhanced by the publication of the Turnbull Report. All businesses should be aware of these guidelines and implement them where appropriate.

## Audit Control

The accounts of the business including all subsidiary companies should be examined by external auditors every twelve months.

## Cash and Receipt Control

All cash and cheques should be banked in full on the day of receipt or next banking day.

Cash in hand and petty cash should be reconciled at least monthly and additionally without warning every six months. Individuals who are not responsible for cash should carry out this check.

## Reconciliation Control

Bank statements receipts counterfoils and supporting documents should be checked at least monthly against cash book entries. Individuals who are not responsible for such entries should carry out this check.

## Cheque Control

All manually prepared cheques or other bank instruments drawn for more than an agreed maximum sum should have two signatures added after the amount has been inserted.

No cheque or instrument should be signed until one signatory has examined the supporting documentation.

For computer or machine prepared cheques or other bank instruments, the supporting documentation should be examined and authorised before the requisition is input. Any computer or machine prepared cheques for an amount in excess of the agreed maximum sum should have one manually applied signature after the cheque or instrument has been prepared.

Of course, the business' bankers need to be told of the arrangements.

### Risk defined:

"Risk management can be described as the culture, processes and organisation that help a business to evaluate risk, assess its potential impact and plan the appropriate action to take in order to avoid or control risk by the most economical means.

It is not possible or desirable to eliminate all risks, the objective is to implement cost effective processes that reduce risks to an acceptable level, reject unacceptable risks, and transfer other risks through insurance and other means."

*Source:*
*Australian Better Business Insurance*
www.aami.com.au/business-insurance

## Payroll

For staff not paid by crossed cheques or credit transfer, the amount of the payroll should be subject to an independent check before payment to ensure that the total amount drawn is correct.

## Stocktaking

A physical check of all stock materials held against verified stock records should be carried out at intervals of not more that 12 months. Individuals who are not responsible for such stock should carry out this check.

## Purchasing Procedures

For all purchases and orders individuals acting independently should be responsible for each of the following procedures;

a) The ordering or authorisation of orders
b) The recording of receipt or certification
c) The authorisation of payment.

## Computer Security

Security checks should be built into all computer functions. Different individuals should be responsible for the authorisation of transactions, the processing of transactions, and the handling of output.

## Investment Control

Investment documents shall be designed to ensure that no one person is authorised to complete a transaction from beginning to end. The business' bankers/stockbrokers need to be told of these arrangements.

## Sales Ledger Statements

Sales ledger statements should be issued at least monthly, direct to customers. Individuals who are not responsible for the receipt of monies should carry out this check. Management need to take action if balances on the sales ledger become three months overdue or are otherwise outside of agreed credit terms.

## Premises Security

All premises occupied in connection with the business should be protected against unauthorised entry. All visitors and contractors should be accompanied by an authorised person for the duration of their visit.

## References

Satisfactory references to confirm the honesty of each new employee who will be responsible for money, goods, accounts, computer operations or computer programming should be obtained.

The references should cover the three years immediately prior to the employment and before a new employee is given responsibility for property.

## Non- Cheque Transfer of Funds

Many businesses now use methods other than cheques to transfer money and, in general, controls in these areas must be similar as those for cheque signing. The value of money transferred by some electronic systems can be very large indeed and strict controls are needed.

As there are so many different methods used we are happy to provide specific guidance on an individual basis.

### Taking a systematic approach to risk

*"Running a business is both exciting and challenging. Every day brings new opportunities and dilemmas, driven by a wide range of factors. The economic climate, changing customer demands, competitor activity and all amongst the variables that can open new doors or precipitate tough decisions.*

*From my point of view, successful business management is about identifying, managing and exploiting risk – being ready for opportunities and challenges, and being able to exploit or deal with them before it's too late. Many businesses could reap huge benefits from a more sophisticated approach to risk management.*

*By taking a systematic approach to identifying, managing and exploiting business risk, many more of the UK's small businesses could build more stable, successful futures. I believe the insurance industry has a significant role to play. Risk management is a core competency for our industry and we have a wealth of risk management skills and expertise at our disposal."*

*- Peter Hubbard, Chief Executive, AXA Insurance*

### Risk Management for SMEs

In October 2002, The Institute of Chartered Accountants in England & Wales (ICAEW) published a paper on Risk Management for the SME sector.

ICAEW has set up a web site collecting together all its resources on risk management and risk reporting and providing links to further information on the topics contained in its paper – www.icaew.co.uk/risk.

The paper suggests that, generally, the four main ways of dealing with risks are grouped as follows:

- accept;
- transfer (usually via insurance);
- reduce/manage; and
- eliminate.

These are sometimes referred to as the four Ts - tolerate, transfer, treat or terminate.

# How Do You Score?

The following questionnaire can be used to gauge the likelihood of a business being surprised by errors or breakdowns that could threaten its future. Mark as applicable: 1 is least applicable, 5 is most applicable.

## Growth:

Pressure for performance:

1
2
3
4
5

Rate of expansion:

1
2
3
4
5

Inexperience of key employees:

1
2
3
4
5

## Culture

Rewards for entrepreneurial risk taking:

1
2
3
4
5

Executive resistance to bad news:

1
2
3
4
5

Level of internal competition:

1
2
3
4
5

## Information Management

Transaction complexity and velocity:

1
2
3
4
5

Gaps in diagnostic performance measures:

1
2
3
4
5

Degree of decentralised decision making:

1
2
3
4
5

Total Score =

Results:

**9 to 20**

**The Safety Zone:**

Businesses that carry this low level of risk are probably safe from unexpected errors or events that could threaten the health of the business. However, managers of such businesses should question whether their risk exposure score is too low. Innovative, successful companies invariably create risk pressure. If your business scores in the safety zone, perhaps it's time to take some calculated gambles.

**21 to 34**

**The Caution Zone:**

Most businesses will find that they fall in this middle zone. But even here, managers should be alert for high scores in any two of the three risk dimensions. For example, if your business scores high on both growth and culture, but the total score falls below 35, there is still reason for concern.

**35 to 45**

**The Danger Zone:**

If you find that your total score is 35 or above, alarm bells should be ringing and fast action should follow. Use the levers of control: belief systems, boundary systems, diagnostic control systems, and interactive control systems - coupled with traditional internal controls - to protect your business from disaster.

*Acknowledgement to and excerpted from:*
*Harvard Business Review May/June 1999*

# Recommended Reading

- *Risk Analysis: A Quantitative Guide* by David Vose published by John Wiley & Sons; 3rd Edition ISBN: 0470512849
- *The Essentials of Risk Management* by Michel Crouhy, Dan Galai and Robert Mark published by McGraw-Hill Professional ISBN: 0071429662
- *The Fundamentals of Risk Measurement* by Christopher Marrison, published by McGraw-Hill Professional ISBN: 0071386270
- *Project Risk Assessment (Successful Business in a Week)* by Donald Teale, published by Hodder & Stoughton General; ISBN: 0340799587
- *Mastering Risk: Part One: Concepts (Financial Times Mastering Series)* by James Pickford (Editor), published by Financial Times Prentice Hall; ISBN: 0273653792.
- *Project Risk Analysis and Management Guide: PRAM*, by Peter, etc. Simon (Editor), published by APM Group; ISBN: 0953159000.
- *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*, by David Vose, published by John Wiley and Sons Ltd; ISBN: 047199765X.
- *Business Continuity Management*, by Dominic Elliott, Ethne Swartz, Brahim Herbane, published by Routledge, an imprint of Taylor & Francis Books Ltd; ISBN: 0415204925.
- *The Definitive Handbook of Business Continuity Management*, by Andrew Hiles, Peter Barnes, published by John Wiley and Sons Ltd; ISBN: 0471485594.
- *Reliability, Maintainability and Risk*, by David J. Smith, published by Butterworth-Heinemann; ISBN: 0750651687.

# The Risk Management Standard

Based on a collaborative work from The Institute of Risk Management, ALARM (The National Forum for Risk Management in the Public Sector) and AIRMIC (The Association of Insurance and Risk Managers).

Risk Management
- External and Internal factors
  Identifies types of risk such as strategic, financial, operational, hazard etc and their external an internal drivers.
- The Risk Management Process
  Identifies the risk management process in tabular form and how it protects and adds value to an organisation and its stakeholders.

Risk Assessment
The overall process of risk analysis and risk evaluation.

Risk Analysis
- Risk Identification
  Identifies and classifies business activities and decisions in a range of ways, including strategic, operational, financial, knowledge management and compliance.
- Risk Description
  Displays the identified risks in a structured format, e.g. using a table to facilitate the description and assessment of risks.
- Risk Estimation
  Estimates risks in quantitative, semi-quantitative and qualitative terms with regard to the probability of occurrence and the possible consequence.
- Risk Analysis methods and techniques
  Identifies a range of techniques that can be used to analyse upside risks, downside risks or both.
- Risk Profile
  Assigns a significance rating to each risk and provides a tool for prioritising risk treatment.

Risk Evaluation
Compares the estimated risks against risk criteria.

Risk Reporting and Communication
- Internal reporting
  Determines what information should be provided to The Board of Directors, Business Units and Individuals.
- External reporting
  Determines information required by external stakeholders.

Risk Treatment
Selects and implements measures to modify risks.

Monitoring and Review of the Risk Management Process
Determines a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

The Structure and Administration of Risk Management
- Risk Management Policy
  Determines the risk management policy including board commitment, assignment of responsibilities and allocation of resources.
- Role of the Board
  Outlines the board's responsibilities.
- Role of the Business Units
  Outlines the business units' responsibilities.
- Role of the Risk Management Function
  Determines the size of the risk management function and its responsibilities.
- Role of Internal Audit
  Determines the responsibilities of the internal auditor who should ensure that the professional requirements for independence and objectivity are not breached.
- Resources and Implementation
  Determines the resources required to implement the organisation's risk management policy at each level of management and within each business unit.

For more information visit www.theirm.org

# Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

## Important Notice

© Copyright 2019, Martin Pollins, All Rights Reserved

This publication is published by Bizezia Limited. It is protected by copyright law and reproduction in whole or in part without the publisher's written permission is strictly prohibited. The publisher may be contacted at info@bizezia.com

Some images in this publication are taken from Creative Commons – such images may be subject to copyright. Creative Commons is a non-profit organisation that enables the sharing and use of creativity and knowledge through free legal tools.

Articles and information contained herein are published without responsibility by us, the publisher or any contributing author for any loss howsoever occurring as a consequence of any action which you take, or action which you choose not to take, as a result of this publication or any view expressed herein. Whilst it is believed that the information contained in this publication is correct at the time of publication, it is not a substitute for obtaining specific professional advice and no representation or warranty, expressed or implied, is made as to its accuracy or completeness.

The information is relevant within the United Kingdom. These disclaimers and exclusions are governed by and construed in accordance with English Law.

Publication issued or updated on: 10 October 2008

Ref: 594