STANDARDS Australia

HB 167:2006

# Security risk management



handbook

HB

STANDARDS NEW ZEALAND
PAEREWA AOTEAROA

# Handbook

# Security risk management

First published as HB 167:2006.



Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7899 2

# Preface

This Handbook was prepared by the following authors for Standards Australia Committee OB-007, Risk Management.

| | |
|---|---|
| Dr Carl Gibson | La Trobe University, Melbourne Australia |
| Mr Gavin Love | International Association of Emergency Managers |
| Mr Neil Fergus | Intelligent Risk Pty Ltd, Sydney, Australia |
| Mr David Parsons | Sydney Water, Sydney Australia |
| Mr Mike Tarrant | Emergency Management Australia Institute, Mt Macedon Australia |
| Insp Mathew Anderson | Counter Terrorism Coordination Unit, Victoria Police, Melbourne Australia |
| Mr James Kilgour | Canadian Centre for Emergency Preparedness, Toronto, Canada |

The authors would like to acknowledge the contributions of all the people involved in the specialist peer review of the Handbook (Appendix A).

The objective of this Handbook is to outline a broad framework and core processes that should be included in a security risk management process, project or program of work.

It is intended that this Handbook can be used by any size or type of organisation—from large multinationals to small businesses, government agencies and the not-for-profit sector—that has identified the requirement for, and merit of, developing effective security risk management processes. However, some recommendations may be more appropriate to some organisation types rather than others.

Many of the apparently technical terms used in security risk management can have subtly different meanings in different organisations. A glossary (Appendix B) has been included to provide consistent definitions as ***they are used in this Handbook***.

The field of security risk management is rapidly evolving and as such this Handbook cannot cover all aspects and variant approaches to security risk management. The authors have endeavoured to provide an overview of both commonly accepted good practices and some promising emerging thinking to inform the understanding (rather than direct) the actions of readers. As such no warranty is provided or implied as to the accuracy or practical applicability of the contents of this Handbook to any organisation or individual.

The extent of the Handbook is based on the broad nature of the security landscape. A range of other security-related Standards Australia publications cover certain aspects at a level of detail beyond the ability of this Handbook to cover, such as IT Security. As such these areas are not considered in detail within this Handbook. A list of other relevant security-related Standards and Handbooks is provided in Appendix C.

This Handbook is consistent with the framework for risk management outlined in AS/NZS 4360:2004, *Risk Management*. Security Risk Management (SRM) plays a critical role as part of an organisation's risk management process in providing a fundamental assessment, control and treatment process for certain types of risk.

Security risk management is a key and fundamental part of an individual's, organisation's or community's wider risk management activities. In a fully integrated risk management system, security risk management should be interlinked at each of its stages with all other risk management activities being undertaken (e.g. financial, safety, marketing, reputation, regulatory, etc). The only real differences are the application of discipline specific knowledge that will occur in each risk management activity – *the overall process remains the same*. Although many of these activities may be conducted by identifiable risk management functions, many may also be conducted as part of the way that other business functions routinely conduct their operations (e.g. employment risk management conducted as a fundamental part of the human resources function).

Risk management provides a key support for decision making providing the means of ensuring that strategy and operations are more appropriately applied. It can, and should, provide an interface between such decision making and the implementation of key functions, processes and infrastructure, which are required to achieve the key personal, organisational or community objectives. Other risk management functions such as business continuity management ensure that the required capability, resources and knowledge are available and accessible to support the achievement of these key objectives.

Security risk management requires fundamentally that the person undertaking it has a thorough understanding of the principles and practice of risk management first and foremost. This must be accompanied by a thorough understanding of security. However, in today's environment, security within an organisation or community cannot stand alone and isolated from all of the other processes and systems.

In contemporary life, security should and must consider and encompass issues such as strategy, governance, ethical conduct, safety and organisational performance. For security risk management to be successfully integrated into the fabric of organisations and society it must become a fundamental aspect of how we all routinely operate. It needs to become a fundamental part of the manager's and community leader's 'toolbag', as much as budget management, communication or decision making skills.

# Contents

*Page*

1 Introduction
- 1.1 Security Risk Management—A new paradigm ..... 6
- 1.2 Security Risk Management Approach ..... 7
- 1.3 Security risk management and its relationship with risk management ..... 10
- 1.4 Security risk management ..... 11

2 Communicate and consult
- 2.1 Introduction ..... 13
- 2.2 Engagement ..... 15
- 2.3 Perception ..... 19
- 2.4 Information transfer ..... 21
- 2.5 Decision making ..... 21
- 2.6 Developing the communications strategy ..... 24

3 Establish the context
- 3.1 Introduction ..... 28
- 3.2 The external context ..... 32
- 3.3 The internal context ..... 34
- 3.4 The security risk management context ..... 35
- 3.5 Determine the process/program structure ..... 36
- 3.6 Developing the evaluation criteria ..... 37
- 3.7 Developing the business case ..... 38

4 Identify risk
- 4.1 Introduction ..... 40
- 4.2 Data and information sources ..... 43
- 4.3 Conducting the criticality assessment ..... 46
- 4.4 Threat assessment ..... 49
- 4.5 Conducting the vulnerability analysis ..... 59
- 4.6 Mapping threat, vulnerability and criticality ..... 66

5 Analyse risk
- 5.1 Introduction ..... 69
- 5.2 Measuring risk ..... 70

6 Evaluate risk
- 6.1 Introduction ..... 77
- 6.2 Tolerance of risk ..... 77

*Page*

7 Treat risk
7.1 Introduction ..... 80
7.2 Developing a treatment plan ..... 80
7.3 Conformance vs. Performance ..... 85

8 Monitor and review
8.1 Introduction ..... 87
8.2 The elements of 'monitor and review' ..... 87
8.3 Monitoring and review practices ..... 88
8.4 Triggering monitor and review processes ..... 89
8.5 Post-event analysis and reporting ..... 90

APPENDICES
A Acknowledgments ..... 91
B Definitions and glossary ..... 92
C Security related standards and handbooks ..... 95
D Sources of data and information for establishing the context ..... 100
E Organisational reference sources for establishing the context ..... 105
F Security risk management workbook ..... 107
G The Admiralty System ..... 145
H Terrorism definitions ..... 146
I Example vulnerability rating matrices ..... 148
J Example components of a security control environment ..... 156
K Community vulnerability assessment ..... 158
L Example questions for use in a vulnerability assessment ..... 161
M Some common approaches to annalysing security risk ..... 163
N Key reference sources ..... 169
O URLs for example reference sources for developing the context ..... 171

# 1 Introduction

## 1.1 Security Risk Management—A new paradigm

'Everything is different', - but it's just the same.

There is a prevailing perception that there have been dramatic and far reaching changes in the nature of the business environment and in society at large over recent years. In particular it has been said, almost *ad nauseum,* that 'the world has changed since 9/11'. However, many of these 'new changes' are merely highlighting issues that have presented challenges to organisations and communities for many decades.

What is different is that this has resulted in a powerful imperative for issues to be now considered that have not previously been part of the collective consciousness. As a society we have been made aware of the need for, and existence of 'security' measures. However, in certain quarters, security has long been viewed as something that people in uniform did whilst guarding *something*. Security belonged in the world of the police, the military or James Bond! When security interfaced with ordinary working lives, we often saw it as hindering our daily routine.

Attitudes have changed significantly in recent times, with a major focus on, and acceptance of the need for, an increased attention to security. However this changed attitude is often driven by misinformed perception, fuelled by an overly dramatic media. The result is that security investment may be misdirected to where the 'noise' is, not where it is really required.

In recent years concepts of organisational risk management have also evolved.

The move has been from the rather simplistic 'risk is insurance mentality' to a more comprehensive enterprise-wide concept that encompasses a better reasoned understanding of the nature of uncertainty that we face. An improved understanding of the nature of risk facilitates more informed decision making, increases our abilities to exploit opportunities and minimise harm.

Similarly, security risk management provides a means of better understanding the nature of security threats and their interaction at an individual, organisational, or community level. Traditionally, the security industry and profession's focus on risk has concentrated on *risk minimisation*, with activities aimed at loss prevention without necessarily thoroughly considering the nature and level of organisational risk.

Some of the key characteristics of this paradigm shift are presented as major themes within this Handbook and are summarised in Table 1.1.