STANDARDS
Australia

HB 167:2006
Security risk management

handbook

HB

STANDARDS
NEW ZEALAND
PAEREWA AOTEAROA

HB 167:2006

Handbook

Security risk management

First published as HB 167:2006.

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

This is a free preview. Purchase the entire publication at the link below:

Product Page