HB 231:2004

Information security risk management guidelines

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND
Paerewa Aotearoa

Handbook

Information security risk management guidelines

Originated as HB 231:2000.
Second edition 2004.

Jointly published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 5649 2

This page left intentionally blank

Preface

The vulnerability of today's information society is still not sufficiently realised: Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. In the business community, for example, most of the monetary transactions are administered by computers in the form of deposit money. Electronic commerce depends on safe systems for money transactions in computer networks. A company's entire production frequently depends on the functioning of its data-processing system. Many businesses store their most valuable company secrets electronically. Marine, air, and space control systems, as well as medical supervision, rely to a great extent on modern computer systems. Computers and the Internet also play an increasing role in the education and leisure of minors. International computer networks are the nerves of the economy, the public sector and society. The security of these computer and communication systems is therefore of essential importance.

European Commission 1998

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities.

OECD 2002

Information security risk management forms the basis for an assessment of an organization's information security framework. With increasing electronic networking between organizations for a very wide range of applications, which impacts on most aspects of life in our society, there is a clear benefit in having a common set of reference documents for information security management. This enables mutual trust to be established between networked sites and trading partners and provides a basis for management of facilities between information users and service providers. Security for information systems is an essential requirement at organizational, national and international levels.

This handbook was revised in 2003 to be consistent with AS/NZS 7799.2:2003.

This Joint Australia/New Zealand Handbook has been prepared by Committee IT-012, Information Systems, Security and Identification Technology. This publication extends the generic work done by Committee OB/7, Risk Management to specifically address the area of information security management. Information security risk management guidelines issued by the International Organization for Standardization (ISO) as ISO/IEC TR 13335*, Information technology—Guidelines for the management of IT security* have been adapted to align with the Australian and New Zealand Standard AS/NZS 4360, *Risk management*.

AS/NZS ISO/IEC 17799 establishes a code of practice for selecting information security controls (or equivalently treating information security risks). AS/NZS 7799.2 (BS 7799.2) specifies an information security management system. Both documents require that a risk assessment process is used as the basis for selecting controls (treating risks). This Handbook complements these Standards by providing additional guidance concerning management of information security risks.

The guidance in this Handbook is not intended to be a comprehensive schedule of information security threats and vulnerabilities. It is intended to serve as a single reference point describing an information security risk management process suitable for most situations encountered in industry and commerce and therefore can be applied by a wide range of organizations. Not all of the steps described in the handbook are relevant to every situation, nor can they take account of local environmental or technological constraints, or be presented in a form that suits every potential user in an organization. Safety critical applications in particular will require additional consideration of factors specific to the circumstances and relevant Standards should be consulted in such cases. Consequently, these guidelines may require to be augmented by further guidance before they can be used as a basis (for example) for corporate policy or an inter-company trading agreement.

It has been assumed in the drafting of these guidelines, that the execution of their provisions is entrusted to appropriately qualified and experienced people.

Contents

1 Scope, Application and Definitions

1.1 Scope

This Handbook provides a generic guide for the establishment and implementation of a risk management process for information security risks.

1.2 Methodology

The risk management process involves establishing the context, identifying, analysing, evaluating, treating, communicating and monitoring of risks.

1.3 Application

Risk management is recognized as an integral part of good management practice. It is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making.

Generally, information security risk management methods and techniques are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful.

This Handbook is intended for use as a reference document by three audiences:

a) managers accountable for the management of information security;

b) personnel who are responsible for initiating, implementing and/or monitoring generic risk management systems within their organizations; and

c) personnel who are responsible for initiating, implementing and/or maintaining information security within their organization.

This Handbook may be applied at all stages in the life of an activity, function, project, product or asset. Often a number of differing studies are carried out at different stages of a project. The maximum benefit is usually obtained by applying the risk management process from the beginning.

This Handbook does not provide sufficient guidance for managing information security risks in safety related systems. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, gives requirements and guidance in this area.