SLOVENSKI STANDARD
SIST BS 7799-2:2003

01-september-2003

Sistemi za upravljanje varovanja informacij – Specifikacija z napotki za uporabo

Information security management - Specification with guidance for use

Ta slovenski standard je istoveten z:

ICS:

35.020	Informacijska tehnika in tehnologija na splošno	Information technology (IT) in general
35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

SIST BS 7799-2:2003 **en**

BRITISH STANDARD

BS 7799-2:2002

Information security management systems — Specification with guidance for use

ICS 03.100.01; 35.020

BSI British Standards

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to BSI-DISC Committee BDD/2, Information security management, upon which the following bodies were represented:

@stake

Articsoft Ltd

Association of British Insurers

British Computer Society

British Telecommunications plc

British Security Industry Association

Department of Transport and Industry — Information Security Policy Group

EDS Ltd

Experian

Gamma Secure Systems Limited

GlaxoSmithKline plc

HMG Protective Security Authority

HSBC

I-Sec Ltd

Institute of Chartered Accountants in England and Wales

Institute of Internal Auditors — UK and Ireland

KPMG plc

Lloyds TSB

Logica UK Ltd

London Clearing House

Marks & Spencer plc

National Westminster Group

Nationwide Building Society

QinetiQ Ltd

Shell UK

Unilever

Wm. List & Co

XiSEC Consultants Ltd/AEXIS Security Consultants

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 5 September 2002

First published as Part 2 February 1998
Revised May 1999

The following BSI references relate to the work on this British Standard:
Committee reference BDD/2
Draft for comment 01/682010 DC

ISBN 0 580 40250 9

Amendments issued since publication

Amd. No.	Date	Comments

Contents

Foreword

This part of BS 7799 has been prepared by BDD/2, Information security management. It supersedes BS 7799-2:1999, which is obsolescent.

This new edition has been produced to harmonize it with other management system standards such as BS EN ISO 9001:2000 and BS EN ISO 14001:1996 to provide consistent and integrated implementation and operation of management systems. It also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing, and improving the effectiveness of an organization's information security management system.

The implementation of the PDCA model will also reflect the principles as set out in the OECD guidance (2002)[1)] governing the security of information systems and networks. In particular, this new edition gives a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in BS ISO/IEC 17799:2000. The list of control objectives and controls in this British Standard is not exhaustive and an organization might consider that additional control objectives and controls are necessary. Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not in itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

[1)] OECD. *OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

0 Introduction

0.1 General

This British Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

This British Standard can be used by internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

0.2 Process approach

This British Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization's ISMS.

An organization must identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs, can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

A process approach encourages its users to emphasize the importance of:

a) understanding business information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls in the context of managing an organization's overall business risk;

c) monitoring and reviewing the performance and effectiveness of the ISMS;

d) continual improvement based on objective measurement.

The model, known as the "Plan-Do-Check-Act" (PDCA) model, can be applied to all ISMS processes, as adopted in this standard. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes (i.e. managed information security) that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses **4**, **5**, **6** and **7**.

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

NOTE The term "procedure" is, by convention, used in information security to mean a "process" that is carried out by people as opposed to a computer or other electronic means.

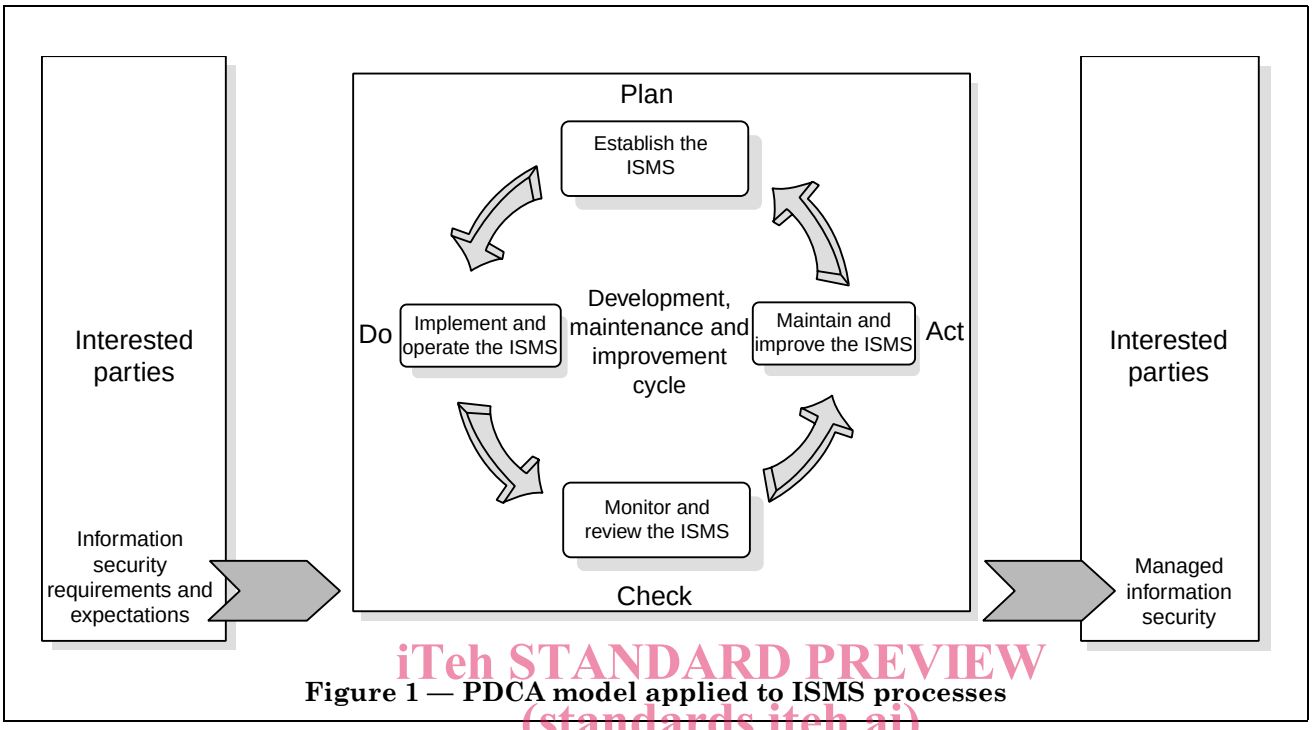

Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the security policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.

0.3 Compatibility with other management systems

This standard is aligned with BS EN ISO 9001:2000 and BS EN ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management standards.

Table C.1 illustrates the relationship between the clauses of this British Standard, BS EN ISO 9001:2000 and BS EN ISO 14001:1996.

This British Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

1 Scope

1.1 General

This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (see Annex B which provides informative guidance on the use of this standard).

The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

1.2 Application

The requirements set out in this British Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature of business. Where any requirement(s) of this standard cannot be applied due to the nature of an organization and its business, the requirement can be considered for exclusion.

Where exclusions are made, claims of conformity to this standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusions of controls found to be necessary to satisfy the risk acceptance criteria need to be justified and evidence needs to be provided that the associated risks have been properly accepted by accountable people. Excluding any of the requirements specified in Clauses **4**, **5**, **6** and **7** is not acceptable.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies.

BS EN ISO 9001:2000, *Quality management systems — Requirements*.

BS ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*.

ISO Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*.

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1
availability
ensuring that authorized users have access to information and associated assets when required
[BS ISO/IEC 17799:2000]

3.2
confidentiality
ensuring that information is accessible only to those authorized to have access
[BS ISO/IEC 17799:2000]

3.3
information security
security preservation of confidentiality, integrity and availability of information

3.4
information security management system
ISMS
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.5
integrity
safeguarding the accuracy and completeness of information and processing methods
[BS ISO/IEC 17799:2000]

3.6
risk acceptance
decision to accept a risk
[ISO Guide 73]

3.7
risk analysis
systematic use of information to identify sources and to estimate the risk
[ISO Guide 73]

3.8
risk assessment
overall process of risk analysis and risk evaluation
[ISO Guide 73]

3.9
risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of risk
[ISO Guide 73]

3.10
risk management
coordinated activities to direct and control an organization with regard to risk
[ISO Guide 73]

3.11
risk treatment
treatment process of selection and implementation of measures to modify risk
[ISO Guide 73]

3.12
statement of applicability
document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes

4 Information security management system

4.1 General requirements

The organization shall develop, implement, maintain and continually improve a documented ISMS within the context of the organization's overall business activities and risk. For the purposes of this standard the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and managing the ISMS

4.2.1 *Establish the ISMS*

The organization shall do the following.

a) *Define the scope of the ISMS* in terms of the characteristics of the business, the organization, its location, assets and technology.

b) *Define an ISMS policy* in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) includes a framework for setting its objectives and establishes an overall sense of direction and principles for action with regard to information security;

2) takes into account business and legal or regulatory requirements, and contractual security obligations;

3) establishes the strategic organizational and risk management context in which the establishment and maintenance of the ISMS will take place;

4) establishes criteria against which risk will be evaluated and the structure of the risk assessment will be defined [see **4.2.1**c)];

5) has been approved by management.

c) *Define a systematic approach to risk assessment*

Identify a method of risk assessment that is suited to the ISMS, and the identified business information security, legal and regulatory requirements. Set policy and objectives for the ISMS to reduce risks to acceptable levels. Determine criteria for accepting the risks and identify the acceptable levels of risk [see **5.1**f)].

d) *Identify the risks*

1) Identify the assets within the scope of the ISMS and the owners of these assets.

2) Identify the threats to those assets.

3) Identify the vulnerabilities that might be exploited by the threats.

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

e) *Assess the risks*

1) Assess the business harm that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risk is acceptable or requires treatment using the criteria established in **4.2.1**c).

f) *Identify and evaluate options for the treatment of risks*

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance [see **4.2.1**c)];

3) avoiding risks;

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) *Select control objectives and controls for the treatment of risks*

Appropriate control objectives and controls shall be selected from Annex A of this standard and the selection shall be justified on the basis of the conclusions of the risk assessment and risk treatment process.

NOTE The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

h) *Prepare a Statement of Applicability*

The control objectives and controls selected in **4.2.1**g) and the reasons for their selection shall be documented in the Statement of Applicability. The exclusion of any control objectives and controls listed in Annex A shall also be recorded.

i) Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

4.2.2 *Implement and operate the ISMS*

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks (see Clause **5**).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in **4.2.1**g) to meet the control objectives.

d) Implement training and awareness programmes (see **5.2.2**).

e) Manage operations.

f) Manage resources (see **5.2**).

g) Implement procedures and other controls capable of enabling prompt detection of and response to security incidents.

4.2.3 *Monitor and review the ISMS*

The organization shall do the following.

a) Execute monitoring procedures and other controls to:

1) detect errors in the results of processing promptly;

2) identify failed and successful security breaches and incidents promptly;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) determine the actions taken to resolve a breach of security reflecting business priorities.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting security policy and objectives, and review of security controls) taking into account results of security audits, incidents, suggestions and feedback from all interested parties.

c) Review the level of residual risk and acceptable risk, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

4) identified threats;

5) external events, such as changes to the legal or regulatory environment and changes in social climate.