

Newly revised BS7799-2:2002

A presentation to the 정보보호 경영시스템 연구회

by 정 성현, BSI Management Systems

shape the future

Introduction

신규격에 포함된 신 개념

- 타규격(ISO9000/14000)과의 조화
- 지속적 개선 / 시스템의 효과성 증대
- 기업 관리 (Corporate governance)
- 정보보호 보증
- OECD Principles 이행

Part2 주요내용

- PDCA Model
- Process approach based on PDCA
- RA, 통제항목 선정, SoA의 정의 및 관계를 명확화
- Annex 에서 신규격의 사용지침을 제공
 - Annex A : Objectives & Controls (Shall)
 - Annex B : 사용지침 (Should)
 - Annex C : ISO9001/14001 & BS7799
 - Annex D : Changes to internal numbering

PDCA

ISMS 유지 및
향상

Plan

ISMS 수립

Action

Do

ISMS 점검 및
검토

Check

ISMS 이행 및
운영

shape the future

Plan

- ISMS Scope 정의
- ISMS Policy 정의
- Risk 식별
- 위험평가
- 통제목표 및 통제 선정
- 위험처치계획 (Risk Treatment Plan) 작성
- SoA 작성

Do

- Resources, training and awareness
- 위험처치계획의 이행
 - Transfer
 - Reduce
 - Accept
- 통제목표를 달성하기 위한 통제의 실현

Check

- 감시절차의 이행
 - Routine checking
 - Self-policing procedures
 - Learning from others
- 계획된 주기로 ISMS 내부감사
- 경영검토의 실시
 - **ISMS** 효과성의 정기적 검토
 - 잔여위험 및 허용위험 수준의 검토
- 경향분석

Action

- ISMS내 부적합의 식별
- 적절한 시정 및 예방조치의 실행

Changes in Controls

- Still alive
- 통제항목은 Annex로 이동 (Normative)
- ISO/IEC 17799와 규격번호 통일

Audit links and trails

- ISMS Policy
- Results of risk assessment
- Security objectives
- Responsibility
- Programmes supporting the ISMS processes
- ISMS procedures
- Performance data
- Security review

OECD Principles

For Security of Information Systems and Networks

- Awareness
- Responsibility
- Response
- Risk assessment
- Security design and implementation
- Security management
- Reassessment

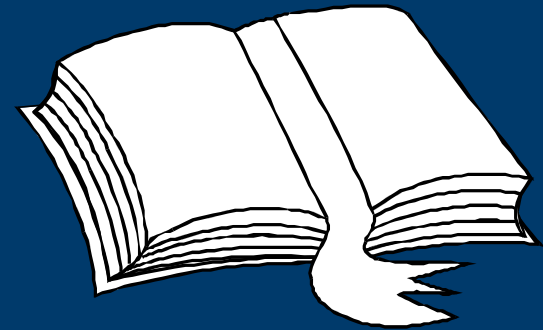
4.2 Scope

- Does the documentation describe unambiguously the scope of the ISMS?
- Are significant exclusions from the scope clearly identified and explained?
- Boundaries/interfaces must be clearly understood (important for the management of customer/supplier/partner relationships)

The management of these relationships is often the most difficult area for consideration in the ISMS.

4.2 ISMS – Security Policy

‘A policy document shall be approved by management, published and communicated, as appropriate, to all employees’



4.3 Documentation Requirements

4.3.1 General

- ISMS shall include:
 - Documented security policy and objectives
 - Scope of the ISMS
 - Risk assessment report
 - Risk treatment plan

4.3 Documentation Requirements

4.3.1 General-contd

- Documents needed for:
 - Effective planning, operation & control
 - Records (4.3.3)
 - Statement of Applicability (SoA) [exclusions shall be recorded]

4.3.2 Control of Documents

Documented procedures shall be established to define the controls needed to:

- Approve documents for adequacy prior to issue
- Review and update as necessary & re-approve
- Changes & the current revision status of documents are identified
- Relevant versions of applicable documents are available at point of use

4.3.2 Control of Documents

- Legible and readily identifiable
- Documents of external origin are identified
- Distribution of documents is controlled
- Prevent the unintended use of obsolete documents
- Apply suitable identification if retained for any purpose

4.3.3 Control of Records

- Records established and maintained to provide evidence of conformity to requirements and to the effective operation of the ISMS shall be controlled
- Records may be manual or automatic

4.3.3 Control of Record

A documented procedure shall be established to define the controls need for:

- Identification, storage, protection, retrieval, retention time, disposition
- Legal requirements need to be considered & overseas?
- Records need to be: legible, readily identifiable and retrievable
- Extent of records – management decide

5 Management responsibility

5.1 Management commitment – Management shall provide evidence of its commitment by:

- Communicating the importance of meeting security objectives, legal & regulatory requirements and continual improvement
- Establishing – security policy, objectives & plans
- Conducting management reviews
- Deciding the level of residual risk

5 Management responsibility

5.2.1 Provision of resources – to:

- Set up and maintain the ISMS
- Security procedures support the business requirements
- Identify & address legal, regulatory and contractual requirements
- Adequate security of implemented controls
- Carry out reviews
- Improve the process

5 Management responsibility

5.2.2 Training, awareness and competency

- Personnel assigned responsibilities in the ISMS shall be competent
- Provide training
- Evaluate effectiveness of training
- Ensure employees are aware
- Maintain records (4.3.3) of education, experience and qualifications

6 Management Review of the ISMS

6.1 General

- Top management shall review at planned intervals etc.

6.2 Review input

6.3 Review output

6 Management Review of the ISMS

6.4 Internal ISMS Audits

- Management shall ensure audits are conducted at planned intervals

7 ISMS Improvements

7.1 Continual improvement

- Seek continual improvement
- Improve the effectiveness of the ISMS through:
 - Security policy
 - Security objectives
 - Results of security reviews
 - Security audits
 - Corrective actions
 - Preventive actions
 - Management review

7 ISMS Improvements

7.2 Corrective action

- Shall take actions to eliminate causes of nonconformities, in order to prevent recurrence
- Documented procedure within the ISMS shall define:
 - Identifying nonconformities
 - Determining the causes
 - Evaluating the need for action to prevent re-occurrence
 - Determining & implementing corrective action
 - Recording the results
 - Reviewing actions for effectiveness

7 ISMS Improvements

7.3 Preventive action

- Determine actions to guard against future nonconformities
- Documented procedure shall define:
 - Identifying potential nonconformities and their causes
 - Determining & implementing preventive action
 - Recording the results
 - Reviewing preventive actions taken
 - Identifying changed risks
 - Ensuring attention on significantly changed risks

감사합니다

BSI Korea

shape the future

