Northwest Controlling Corporation Ltd.
Internet: http://www.noweco.com/
Email: info@noweco.com

The Information Security Management System of BS 7799-2:2002

The Management System for ISO 17799

by Andreas E. Fiedler

Introduction

The publication of the standard ISO 17799 provides an international basis for a common understanding of management of information security. ISO 17799 was developed as a standard containing codes of practice for information security management to ensure that appropriate action is taken to secure data storage and transfer - whether data is provided in paper or in electronic form.

ISO 17799 "Code of Practice for Information Security Management" refers to ten control for these actions:

- Security Policy
- Security Organisation
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

After the framework for managing information security is given this way a question arises about the management system which shall perform the management of information security. How does such a management system look like?

BS 7799-2:2002

The standard ISO 17799 was made from British Standard BS 7799. Whereas BS 7799 contains two parts ISO 17799 only took over the first part of BS 7799.

BS 7799-2 is concerned with the management system. The standard mentions four major areas:

- Information Security Management System (ISMS)
- Management Responsibility
- Management Review
- ISMS Improvement

From the perspective of management the four areas can be merged into two blocks:

- the management control system comprises documentation, audit and review, responsibility of management, corrective and preventive action and continuous improvement.
- The information security management integrates the processes of the PDCA cycle to establish, implement, operate, monitor, review and improve the ISMS.

The Information Security Management System

Overview

The PCDA (Plan-Do-Check-Act) model used as basis for the revision of BS 7799-2 was not only selected to conform to other management standards such as ISO 9000 or ISO 14000. It even more emphasises a strict process thinking to use this model which has its root in quality management.

The phases or activities of the PDCA cycle are:

- PLAN: Establishing the ISMS
- DO: Operating the ISMS
- CHECK: Monitoring and reviewing the ISMS
- ACT: Improving the ISMS

PLAN

The PLAN phase is concerned with establishing the ISMS. The first step is to determine the scope of the ISMS, i.e. responding to what shall be controlled by the ISMS. An ISMS policy has to be defined that includes objectives, legal or regulatory requirements, contractual obligations, strategic organisational and risk management context and risk assessment criteria.

There has to be a systematic approach to risk management. The definition of such an approach can be assisted by the very famous standard AS/NZS 4360:1999 from Australia and New Zealand or a standard published in the UK: AIRMIC, ALARM, IRM:2000.

Note: This standard is jointly developed by The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM The National Forum for Risk Management in the Public Sector.

In context of ISMS risk management consists of six steps:

1. Risk Identification
   This step identifies the assets becoming subject to risk assessment and threats to those assets. Further vulnerabilities that might be exploited by the threats and potential losses have to be identified.
2. Risk Assessment
   Risk assessment means to look at typically two parameters: probability of occurrence of risk and impact in case of occurrence of risk.
   The FMEA (Failure Mode and effects Analysis) provides a third very interesting parameter: the probability of detection. This is the probability that the

occurrence of a threat is detected by using detection actions before any major impact has happened. An example for detection actions are virus scans or intrusion detection.

3. Action Identification and Assessment
   There are several options of how to respond to a risk, including:
   - taking actions
   - accepting risks
   - avoiding risks
   - transferring risks to other parties.

4. Controlling Risk Actions
   ISO 17799 includes several controls without claiming these to be complete. These controls shall be selected and justified on basis of the results of risk assessment.

5. Statement of Applicability
   The Statement of Applicability documents the controls.

6. Management Approval
   Management has to approve the implementation of the ISMS. The responsibility of management is a key success factor for the ISMS (please cf. below).

DO

The DO phase implements the steps as planned in the previous phase. Activities as known from project management are employed to build the ISMS. These include:
- Management of implementation
- Resource Management
- Schedule Management
- Training Management

CHECK

In the CHECK phase the ISMS is monitored and reviewed.

1. Monitoring
   Monitoring the operation of the ISMS includes detecting errors in the results of processing, identifying security breaches, auditing performance, identifying actions taken to resolve a security breach, following up actions in case of security breaches.

2. Review
   Reviews ensure the effectiveness of the ISMS; they are conducted in a regular manner. Reviews include:
   - Security Policy and Objectives
   - Audits
   - Observations
   - Suggestions for Improvement
   - Feedback

3. Residual risk
   Residual and acceptable risk has to be reviewed regularly with regard to impact on organisation, technology, business objectives and processes, identified threats and external effects such as legal or regulatory environment and changes in social climate.

ACT

The ACT phase is the phase of improvement. In this phase improvements are implemented, corrective and preventive actions taken, results communicated with all interested parties and improvement actions monitored.

The Management Control System

The management control system comprises:

- Document Control
- Audit
- Review
- Responsibility of Management
- Corrective and Preventive Actions
- Continual Improvement

Document Control

Document Control of ISMS is the same as of quality management. Hence, all organisations having implemented a document control system conforming to ISO 9000: 2000 will meet the requirements of BS 7799-2 with regard to the procedures needed for document control. The single steps are:

- Approval of documents for adequacy prior to issue
- Review and update of documents as necessary and re-approve
- Identification of changes and current document revision status
- Availability of relevant versions of documents at points of use
- Legible and readily identifiable documents
- Identification and controlled distribution of external documents
- Controlled distribution of documents
- Prevention of unintended use of obsolete documents
- Suitable identification to obsolete documents if they are retained.

BS 7799-2 lists documents to be included into the ISMS:

- Statements of security policy and control objectives
- Scope, procedures and controls of the ISMS
- Risk assessment report
- Risk treatment plan
- Procedures to ensure the effective planning, operation and control of its information security processes
- Records (cf. below
- Statement of Applicability

Control of Records

Records have to be made and maintained as evidence of conformance to the standard and to demonstrate the effective operation of the ISMS. Again, the requirements are the same as for quality management.

The procedure to control records has to be documented and comprises:

- Identification
- Storage
- Protection
- Retrieval
- Retention
- Disposition

The internal Audit

The internal audit plays a core role in the effort of maintaining information security and improvement. Audits shall ensure that all elements of the ISMS conform to the requirements of the standard and identified information security requirements, are effectively implemented and maintained

and perform as expected. The results of audits are:

- Actual, detected concerns (cf. below: Corrective Actions)
- Potential concerns (cf. below: Preventive Actions)
- Opportunities for improvement (cf. below: continual improvement)

Audit activities comprise:

- Definition of audit objectives
- Examine the documents
- Audit planning
- Auditing
- Audit results report
- Completion of audit plan
- Follow-up audits as needed

Organisations running a quality management system easily can combine the audit function of the ISMS with the one of quality management.

Management Review

Management has to conduct a management review of the ISMS; this again is known from quality management. The management review shall confirm the continuing suitability, adequacy and effectiveness of the ISMS.

Review input includes audit and review results, corrective and preventive actions, recommendations for improvement and new technologies and procedures.

The results of a review are corrections and improvements to the ISMS and provision of resources as needed.

Management Responsibility

A very important, though often neglected element of the management control system is management responsibility. It covers three items:

- Management commitment
- Resource management
- Training, awareness and competency

Management Commitment

Management commitment is like in other management systems a critical success factor. In particular, management has to care about:

- Establishing the information security policy
- Ensuring that information security objectives and plans are established
- Assigning roles and responsibilities
- Communication of importance of information security
- Providing sufficient resources for the ISMS (cf. below)
- Deciding about acceptable level of risk
- Conducting management reviews

Resource Management

Management is responsible to provide sufficient resources to:

- Establish, implement, operate and maintain the ISMS
- Ensure that ISMS procedures support the business requirements
- Ensure that legal and regulatory requirements and contractual obligations are addressed
- Ensure adequate security by applying implemented controls
- Carry our reviews and taking appropriate actions

- Improve effectiveness of ISMS

Training, Awareness and competency

Management is responsible that all personal of the ISMS is sufficiently trained. In detail:

- Determining necessary competency
- Providing training
- Evaluating effectiveness of training
- Maintaining training records experience, skills and qualifications.

Corrective and Preventive Actions

Internal audits and other internal and external source provide evidence about the effectiveness of the ISMS. Actions are initiated to eliminate any concern and prevent the re-occurrence of such concern. With regard to the management system there are two important types of actions: corrective actions and preventive actions.

Corrective actions are actions taken after the occurrence of a risk or a concern to prevent re-occurrence in the future.

Preventive actions are used to anticipate potential risks or concerns and to prevent any potential future damage before any occurrence is detected.

Continual Improvement of the ISMS

Both ISO 9000:2000 and BS 7799-2 list next to the just mentioned corrective and preventive actions the continual improvement. Whereas corrective and preventive actions focus on detected or potential concerns actions also can be taken to further improve a system in terms of effectiveness and efficiency that is free of any concern.

The continual striving for improvement without being based on any problem or concern is very important for any successful management system. It is the step from a re-active to a pro-active management.

The steps of continual improvement are:

- Identification of possible improvement areas
- Analysis and justification of needed action
- Determining availability of resources
- Deciding to implement improvements
- Implementing improvements
- Measuring impact on organisation
- Considering results at management review
- Continually looking for improvements

Conclusion

BS 7799-2 provides an information security management system to realise information security as determined in ISO 17799. The neighbourhood to ISO 9000 is obvious and an important issue to efficiently setup the system.

BS 7799-2 is a fundamental add-on to ISO 17799 as it allows to integrate information security actions in a management system. Such a management is the basis any success in information security.

BS 7799-2 provides organisations with the opportunity register the ISMS and communicate the own commitment. ISO 17799 does not serve this.