On the necessity of management of information security

The Standard ISO17799 as international basis

by Andreas E. Fiedler

Introduction

Information in an organisation is the available organisational knowledge. It contains the organisational experience of the past as well as the organisational potential of the future. Information is the critical success factor no. 1. Vice versa, threats to information or information mediating procedures are threats to quality, effectiveness and finally organisational existence per se. Information security (IS) is the response to the risks organisational information is facing.

Management of Information Security

In most information systems information security is not given a priori. Technical solutions for themselves are limited in their effectiveness and require management assistance.

The system view established by quality management (Plan - Do - Check - Act), also known as Deming Wheel, is a principal method for any management system. It can also be applied for information security management systems.

Starting point for planning is an inventory or an audit of the current system. These are confronted with the security requirements. Source for this are the identification and analysis of risks, legal and contractual requirements, and organisation-internal practices. Actions can be derived from the security requirements which shall be implemented. According to quality management it is important to audit the success of any actions taken and whenever necessary to identify appropriate corrective action. Management of information security is not static but a continuous process.

The Standard ISO17799

In 1995 the British Standards Institution developed British Standard BS7799 which should provide recommendations on how to design an information security management system (ISMS). The success of this standard was great so that it is now internationally accepted and published as ISO17799.

It is important to note that the standard ISO17799 is not intended to have a normative as ISO9000 on quality management is so often misunderstood. In the foreword to Part 1 it is stated that the standard "takes the form of guidance and recommendations": Further, "it should not be quoted as if it were a specification, and particular care should be taken to ensure that claims of compliance are not misleading"[1]. The textual benefit of a code of practice takes priority.

The Benefits of an international Standard

The International Organisation of Standardization describes the benefits as follows: "ISO/IEC 17799 transforms the British Standard BS 7799, which has been adopted in many countries, into an International Standard and it is expected to become the reference document for codes of good practice to ensure secure and trustworthy e-commerce."[2]

The 10 Controls of ISO17799

ISO17799 comprises ten controls on which actions shall be taken to ensure meeting their objectives. The controls are:

Security Policy

Management defines in their security policy a strategic direction for information security and demonstrates support and commitment. The security policy, both documented and applied, is a core requirement for the success of the ISMS.

Security Organisation

The organisation of security means principles and procedures to manage information security. These also include security of third party access and outsourced information processing.

Asset Classification and Control

To protect information assets there first has to be made an inventory of all information assets given in an organisation. A classification of the information assets helps to characterise these and assign appropriate protective actions.

Personnel Security

It is the objective of personnel security to reduce the risks of human error, theft, fraud or misuse of facilities.

User training is a very important focus of personnel security to establish an understanding for information security and encourage an according behaviour. This also includes training in responding to security incidents and malfunctions.

Physical and environmental security

Secure areas prevent unauthorised access, damage, and interference to business premises and protect against loss, damage, compromise of assets and interruption to business activities.

Communications and Operations Management

This control area serves (a) to ensure correct and secure facility management of information processing, (b) to mitigate the risk of systems failure, (c) to protect information and software integrity, (d) to ensure integrity and availability of information processing and communication services, (e) to protect information security in networks and supporting infrastructure, (f) to prevent damages to assets and ensure on-going business activities, and (g) to prevent loss, modification or misuse of information that is shared between organisations.

Access Control

Access control determines access to information systems. Unauthorised user access, computer access, access to information shall be prevented Network services shall be protected. Further some focus is put on mobile computing and teleworking.

Systems Development and Maintenance

Already during development of systems consideration must be given to sufficient security. In application systems loss, modification or misuse of user data shall be prevented. Cryptographic controls help to protect the confidentiality, authenticity, and integrity of information. Generally, IT projects and support activities shall be conducted in a secure manner.

Business Continuity Management

Corrective and preventive action shall be taken to prevent interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Compliance with Legal Requirements

The last of the ten controls focuses on avoiding breaches of any criminal and civil law, and statutory, regulatory or contractual obligations as well as any security requirements. Further organisational security policies and standards shall be met. Audits of the ISMS shall be planned and agreed to mitigate the risk of disruptions to business processes.

Establishing a Management Framework

With the adoption of British Standard BS7799 into ISO17799 only the first part of BS7799 "Code of Practice for Information Security Management" became an international standard. However, BS7799 includes a second part named "Specification for Information Security Management Systems" which contains some additional information. The most significant is the section on how to establish a management framework.

At this point it shall be noted that this management framework is nothing but a risk management system which should be given in any organisation in order to meet the phenomenon of uncertainty. With regard to managing information security BS7799, Part 2 asserts six steps.

1. Definition of the Security policy
   The management framework of the ISMS requires a policy like any other management system to define strategy, objectives, intentions and responsibilities.

2. Definition of the Scope of the ISMS
   This means the description of the boundaries in terms of the characteristics of the organisation, its location, assets and technology.

3. Risk Identification and Analysis
   In this step threats to the assets, vulnerabilities and impacts on the organisation are identified and the risk is evaluated (typically probability and impact in case of risk occurrence).

4. Risk Management
   The areas of risk need to be identified based on the required degree of security within the security policy.

5. Selection of Control Objectives and Controls to be implemented
   With regard to the risk areas identified in the step before control objectives and controls for implementation have to be selected.

6. Preparation of a Statement of Applicability
   The selected control objectives and controls including the reasons for selecting these are documented in the statement of applicability.

Registration to BS7799 Part 2[3]

The same way organisations can be registered after the quality management standard ISO9000 they can be registered after BS7799 Part 2[3]. The benefits of registration are:

- Confidence, trust and credibility
  Customers and other stakeholders gain confidence that information from them and about them is secure and protected.

- Saving costs
  The cost of only a single information security breach can be significant. Registration reduces the risk of such security breaches through external specialists auditing the system.

- Compliance with laws
  Registration to BS7799 Part 2 demonstrates compliance with all relevant laws and regulations.

- Commitment
  Registration demonstrates commitment on all levels of the organisation.

Continuous Improvement of the ISMS

Management systems are nothing sporadical but a continuous process that focuses on ensuring achieved levels and permanently improving these. The principle of continuous improvement which is known in quality management is valid also for the ISMS. Within the ISMS it is the goal to preserve the achieved security standard by responding to new security threats. Finally, it means to close still existing security gaps and improving the ISMS this way.

The critical success factor of managing information security is the identification of weaknesses or sources of risks. The tool used for gap analysis is the audit. An audit compares the actual performance with the planned or targeted one whereby the target is mirrored in the standard ISO17799 or its further development done specifically by each organisation.

The identified risk can then run through the typical risk management process. This means they are evaluated in terms of probability of occurrence and impact in case of occurrence. The risk factor resulting from these is the value to prioritise which risks to take care about first.

Candidate actions have to be identified for the risks to mitigate their probability and/or impact. Candidate actions showing the highest effectiveness and highest cost efficiency will be selected for implementation.

A follow-up audit can determine the success which is achieved by the implementing appropriate actions.

The complete risk situation with regard to information security within an organisation can be simulated by using the Monte Carlo Analysis. The mean of the overall risk costs resulting from Monte Carlo Analysis is in most cases significant and can excellently serve as motivation to establish and maintain a systematic management of information security.

Revision of BS7799 Part 2

Having the success of the quality management standard ISO9000 in mind it is not surprising that elements from the one management system will be adopted by the other one. This adoption takes place with the revision of the second part BS7799:1999 meaning the part being relevant for registration after BS7799. The harmonisation with ISO9000 concerns in particular:

- The Plan-Do-Check-Act model
- The process focus
- Definitions and explanations
- Corresponding sections in the standards ISO9000 and BS7799 Part 2

Conclusion

Information is already recognised as critical success factor both in the private and public sector. Hence, information needs to be protected and kept secure. Just looking for technical approaches is not sufficient. Without a systematic management of information there can be not effective protection. ISO17799 now is an international standard that can serve as basis for a "best practice" and can globally be communicated. Registration after BS7799 Part 2 will especially help those organisations that want to demonstrate to customers and other stakeholders that confidentiality, integrity, and availability are always ensured.

Literature

[1]**ISO17799:** International Organisation of Standardization

[2]**Standards of 2000:** published at the website of the International Organisation of Standardization

[3]**BS7799, Part 1 and 2**: British Standards Institution