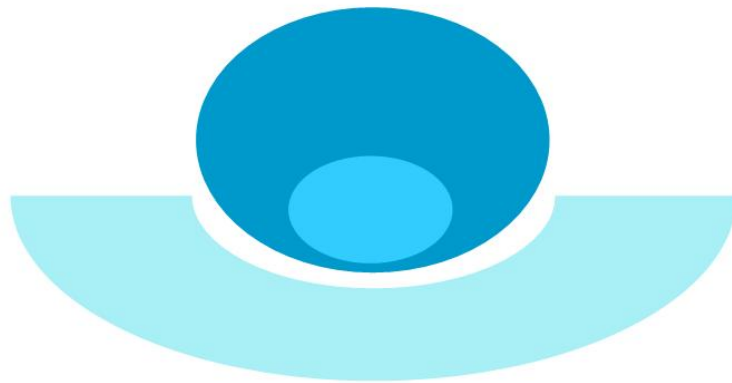




Heikki Mäkinen

For Development of ISMS Standards



**Version 1.0
7.4.2006**

Knowledge of Society White Paper : 4

This Document is OBSOLETE

**Superseded by
[The Social Foundations of Information Security](#)**



Heikki Mäkinen

For development of ISMS standards

Process approach and ISMS

Information Security Management System (ISMS) standards (standard series ISO/IEC 27000) are under development process. This is the most important process going on in information security development of modern society, and a very important process for even the development of Information Society.

The planning approach of the standard has changed substantially since the first appearance of BS 7799 'Code of Practice' standard in 1995, the ancestor of ISMS-standards. The first versions were directed to a building of an information security plan, a document. ISO 27001 and ISO 17799:2005 have clearly adopted the process approach to the development and improvement of ISMS.

But there is always the next step. In recent standards process approach is concentrated on the development and improvement process of ISMS. It is not part of the definition of assets and concerns only partly the operations of ISMS. ISMS is not thoroughly analysed as a process organisation.

The starting point of process approach is to analyse the organisation according to its results, products or services it is producing, but not according to for example the division of labour in organisation, its hierarchy or sectors of information processing system.

ISMS is aimed to protect assets which are resources of the value creating processes of the organisation. Assets should be analysed from the point of view of this value creating process. This means that there should be a process and knowledge to protect the assets in a way value creating process presupposes.

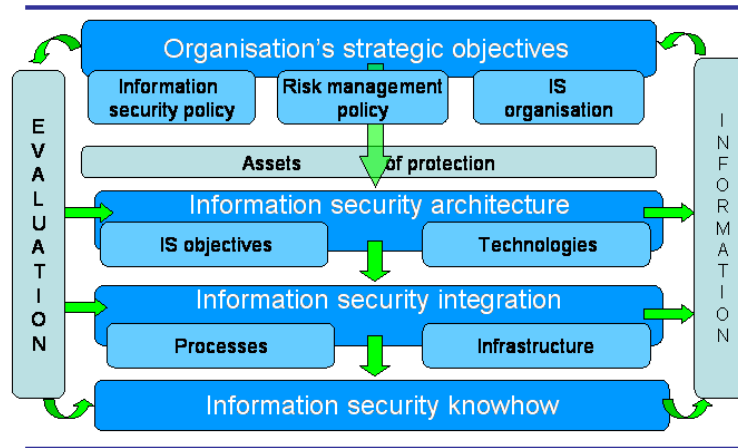
Knowledge Management and ISMS

Process approach to the management of organisation is a subspecies of a more general management approach: Knowledge Management¹. In my opinion ISMS is a Knowledge Management system. There is defined a process for creating information security knowledge and a process for managing that knowledge. The former defines objectives and measures and the latter feedback of them to the management's review. Information Security know-how is created (by processes of human resources security) as means of implementing ISMS. ISMS can be described as follows:

¹ "Knowledge management may become the most universal management concept in history" (Takeuchi, 2001, 328).



Information Security Management System



This interpretation of ISMS specifies the starting point in organisation's strategic objectives which define information security policy, risk management policy and information security organisation. These are defined for a set of assets chosen to define the scope of ISMS.

Through information security evaluation process is defined information security architecture which defines security objectives and requirements for assets and technology used to reach them. These objectives, and measures developed to fulfil them, are applied in organisation's value creation processes and infrastructure which is the environment of these processes. This presupposes development of information security know-how in organisation.

About all information security activities is gathered information which is reported to the management. Management's responsibility is to make corrective actions in the functioning of ISMS (Mäkinen, 2005a, 26 - 37, Mäkinen, 2005b).

In a similar way can be described the risk management system. Starting point is organisation's strategic objectives. These define the emphasis and priorities of risk management and the assets which are important from the point of view of risks.

Risk assessment consists of identification and description of threats and vulnerabilities of systems, activities and technology. Every threat and vulnerability is described by its cause and consequences. Risk is threat or vulnerability for which has been defined probability and consequences. These must be measurable. The information created in this process defines the measures against risks. These are reported to the management's review (Mäkinen, 2005a, 44 – 54, Mäkinen, 2005b).

Results of audit, compliance analysis, information security incident management and results of risk analysis may all be handled as part of ISMS's information managing process reporting to the management's review

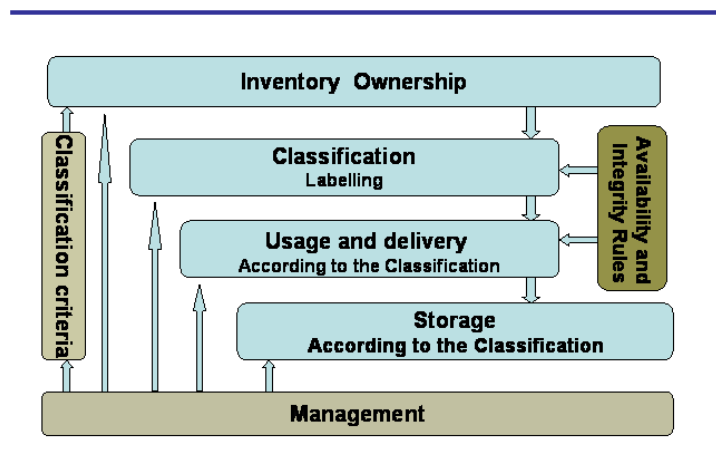


Security Management of Assets

Assets are the objects of ISMS. Control objectives and controls which are intended to management of assets' security, can be seen as a management processes. These should be part of every value creating process. Management should be done in a general way, defined by information security policy and security objectives concerning the asset, in every process.

This can be described for example by the process of information assets management.

Information assets management



The same management process can be applied in every case where information has an external carrier. It can be applied in description of assets management (responsibility for assets, information classification, ISO 27001, A.7.) as when discussing media handling (A.10.7) as part of communications and operation management.

Information asset is however only one form of knowledge. Knowledge is divided into explicit and tacit knowledge. The latter is always bound with the human action and necessarily has no external carrier. 'Knowledge asset' is developed from human knowledge (Mäkinen, 2005a, 20, Nonaka – Toyama – Konno, 2001, 33). The process of organisation's information/knowledge management system should consider also knowledge assets. This presupposes analysis of items which in standard belong to the category 'Human Resources Management'.

External parties, external services

External relations of organisation are considered in several sections of standard, for example:

- Information security organisation (6.2. External parties),
- Operations management (10.2. Third party service delivery management),



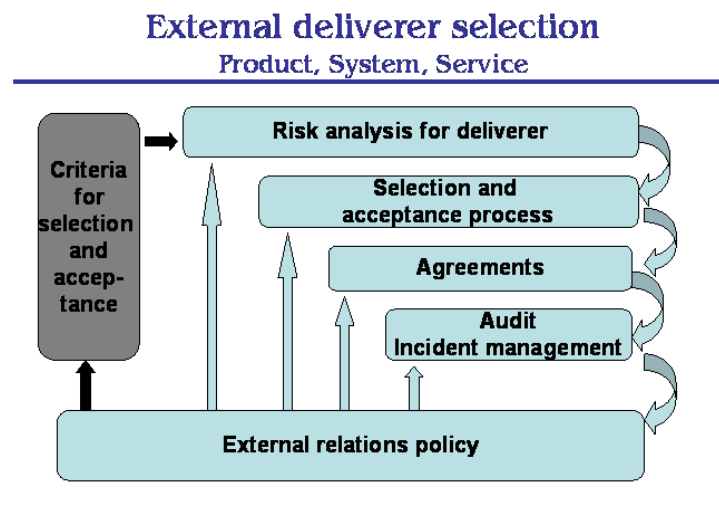
- Network security management (10.6),
- Agreements with exchange of information (10.8.2),
- Network access control (11.4. 1),
- Acquisition of information systems (12.1) and outsourced system development (12.5.5).

It seems to me that organisation should have a general process for management of External relations and these relations should be considered as a specific asset. This is relevant also because the environment, where organisation are working, is in modern society always networked.

External relations have several roles from the point of view of organisation. The main roles are: is organisation buying or selling. If buying, organisation must make a selection process of service or product supplier and an agreement. If selling, situation is different if customer has some kind of access to the network of organisation - selling of a service - which is managed by an agreement and a specific access management policy. The other case is selling a product when the external relation is simply an agreement.

Also the type of external relation is meaningful. There are two types: relations between two or several known parties and relations to a general, public network or social service. The latter is concerned for example in relation to electronic commerce (10.9.1).

Acquisition of product, information system or service can be described as a selection process as follows:



The starting point of external relations management is definition of required service and information security level. This can be done in a specific external relations policy. It defines also these relations and roles they have (buying, selling, agreement parties, general relationships) and specific policies, instructions or processes followed in different lines. Also principles of agreements, which are part of every external relations



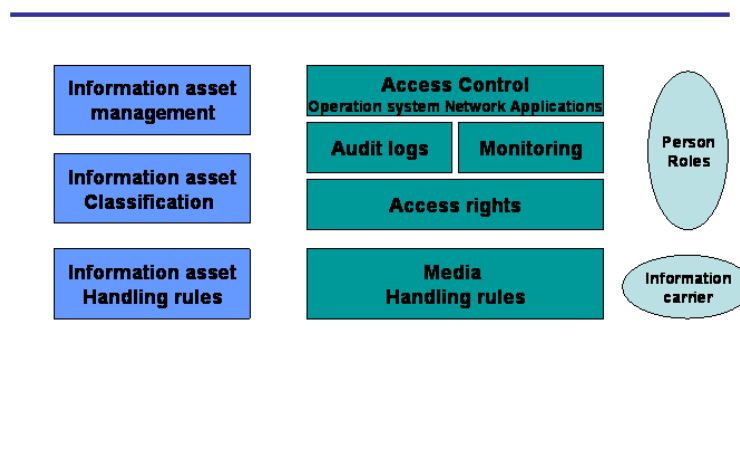
process, and situations when risk analysis is done, should be specified in policy. Further the criteria for deliverer or supplier selection and acceptance should be in policy. The actual selection and acceptance process should define tasks, responsibilities and information gathered about deliverer.

Follow-up of service and information security level and incidents are also very general objects in external relations management. The procedure and methods for accomplishing this and information gathering should be defined.

Access control

Access control is in standard a specific asset controlled by an access control policy (11.1.1). In practice standard however considers access control separately in network, operation systems and applications; a special consideration is for teleworking and customer relationships too. It should be possible to consider also access control as a unified process governed by rules of information assets management and access control policy. Important is that - as a result of access control - information is handled according to the security rules attached to it, not according to its information in network, operation system, in application or at the teleworking place.

Access Control Processes



There should be a general process of access control which includes definition of confidentiality of information assets, user access rights to assets, monitoring of assets' use and their handling according to confidentiality, availability and integrity rules in information processing facilities and in external carriers (like document, file, database, screen, speech). The actual control process should consist of responsibilities for defining access rights according to information classification.

Communications and operations management

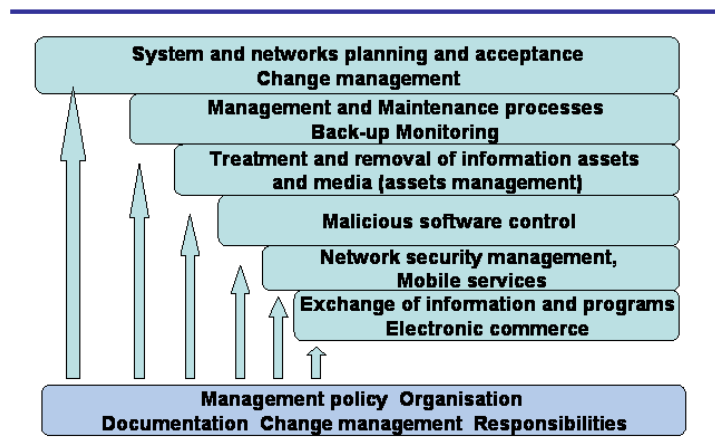
In standard 'Communications and operations management' is considered in a quite same way as 'Access control': it is defined as an asset to be protected but analysed



according to the specific sectors of information processing. Interesting for user is however the results of management process – which includes several subprocesses - from the point of view of organisation's activities.

The standard describes following processes of communications and operation management (ISO 27001, A.10, ISO 17799, Ch. 10):

Communications and Operations Management Processes



It would be useful to consider system and networks environments from three different points of view according to the result activities - especially networking - is aiming for:

- environment of one organisation,
- agreement environment of several known organisations,
- general, public environment (ECMA-271).

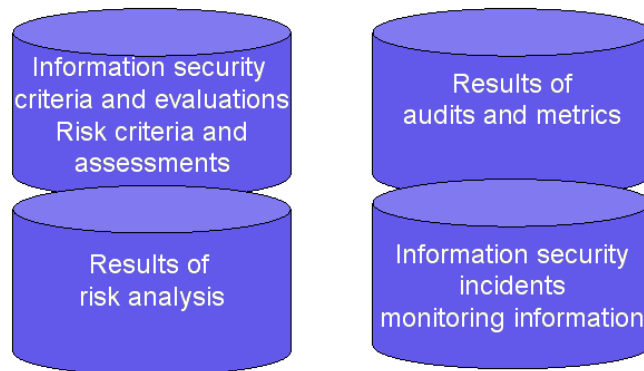
The basics of management processes are same regardless of the environment; information security is always constituted of the activities of organisations and users. But when it is discussed of environments where are external parties or general networking environments these relationships should be specified as specific assets.

Information management

Information security Information/Knowledge management has a central role in standard. It is also considered in several places. Information management should result in a central co-ordination of information security information. Based on this are prepared reports and proposals for management's review. Information should be arranged in a database.



Information on information security



This database consists of:

- Information security and risks assessment criteria and evaluations
- Results of risk analysis
- results of audits and metrics
- Information security incidents information.

Information gathering and reporting should be defined as one formal process for ISMS information creation, reporting and improvement.

Literature

- ECMA, European Computer Manufacturers Association: Extended Commercially Oriented Functionality Class for Security Evaluation, ECMA-271, 1997 (www.ecma-international.org)
- ISO/IEC, International Standardisation organisation, Standard 27001: Information Technology - Security techniques- Information Security Management Systems – Requirements (2005-10-15)
- ISO/IEC, International Standardisation organisation, Standard 17799: 2005: Information Technology - Security techniques. Code of practice for information security management, Second Edition (2005-06-15)
- von Krogh, Georg – Ichijo, Kazuo – Nonaka, Ikujiro: Enabling Knowledge Management. How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation. Oxford University Press, 2000
- Mäkinen, Heikki: Yhteiskunnan tiedon turvallisuus (in Finnish), 2005a, www.yhteiskunnantieto.fi
- Mäkinen, Heikki: Knowledge of Society: Security. Central arguments. (Summary of ‘Yhteiskunnan tiedon turvallisuus’), 2005b, www.yhteiskunnantieto.fi.
- Nonaka, Ikujiro – Teece, David J. (eds): Managing Industrial Knowledge. SAGE Publications, London, 2001



Nonaka, Ikujiro – Toyama, Ryoko – Konno, Noboru: SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. In Nonaka – Teece, 2001
Takeuchi, Hirotaka: Towards a Universal Management Concept of Knowledge. (In Nonaka-Teece, 2001)