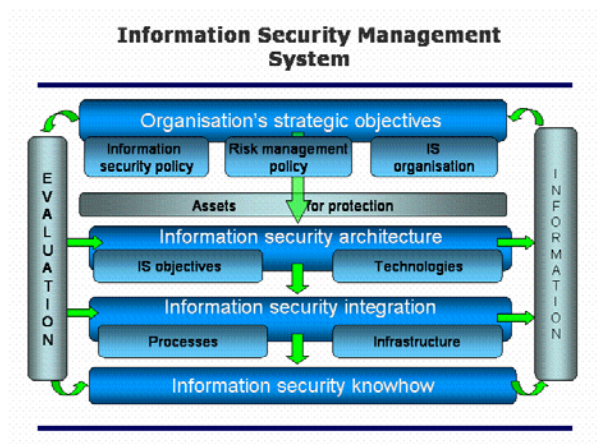


Information Security Management System Development

Information Security Management System (ISMS)



Standard series ISO 27000 defines Information Security Management System (ISMS). It does not however define the exact structure of the system. This is on responsibility of the application.

Information security management system includes following parts:

- information security policy, risk management policy and definition of information security organization according to strategic objectives of action,
- information security architecture and requirements,
- application of former topics in practice through process integration and information security know-how,
- processes for information security evaluation, security information management and its reporting to the management.

Information Security Management System is according to the standards specified for organization. Management of information security builds in social division of labour organization and in network environment information society service. Organization is a historical social formation. The foundation of social relationship is interaction based on knowledge relation. Organization is its special form. Social relationships are developed from management of global risks. Information security is a principal factor at social

(Mäkinen, 2008, Mäkinen, 2008/12, Mäkinen, 2008/13, Mäkinen, 2009/14).

Information security management system must be specified also for processes and information society services (Mäkinen, 2009/10, Mäkinen, 2009/11). In both cases the foundation is definition of information security architecture for assets to be protected

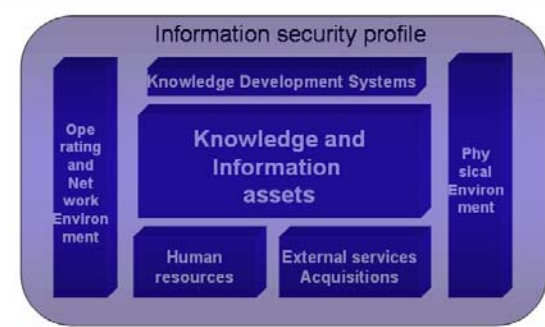
Assets (of protection)

Information security is directed on foundation of valuable assets. These specify the scope where information security management system is applied. Organisation and information society service must make an inventory of assets and define their value.

Assets to be protected are according to ISO 27000 standard:

- knowledge and information assets,
- operating and network environment which consists of communications networks and services, information systems, programs and equipment,
- physical environment,
- human resources,
- external parties services and acquisitions.

Assets for Protection



The most essential objective of protection are information assets. When connected to person and activity they include also tacit knowledge and knowledge assets defined according to it.

Operating and network environment and physical environment together form the environment where knowledge is produced, transferred and stored. Information security is integrated into this environment.

Information Security in Value Creating Processes and Networks

The other objective where information security is integrated is value creating processes and network they build. There actually is produced knowledge with methods conforming with generally accepted information security principles.

In process and network the basic productive unit is service, instead of organization. It does not have a constant social structure but the connection of global and historical dimension of social is built on foundation of information security. In organization's processes this is supported by structures of organization but in network, information society service, information security is the only factor determining social.

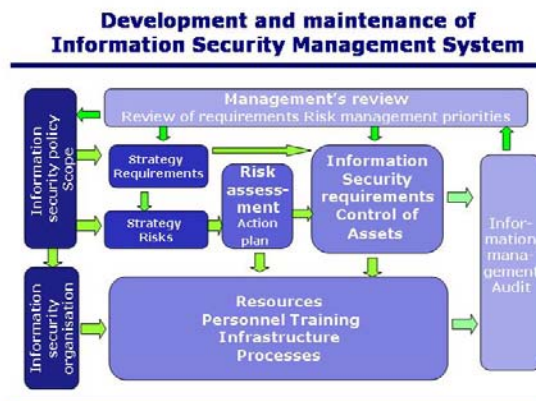
Information Security Management System Development Process

Information security management is a formal management system. Its development process must be defined. This process is at the same time the maintenance process of management system.

Standard ISO 27001 defines development of information security management system by principle of continuous improvement. Process constitutes of phases: Plan, Do, Check and Act (PDCA).

The practical information security tasks specified by this principle determine the phases of development process as projects. Starting point of development process is definition of information security policy and organisation. Information security policy is concretized in strategy plans of information

security requirements and risk management. According to risk assessment are defined priorities of detailed instructions and order of development.



Process is resourced according to organization. About implementation is gathered information which is starting point for management's review. According to this are revised information security policy and strategies if required.

Literature

ISO/IEC, International Standardisation organisation, Standard 27001: Information Technology - Security techniques- Information Security Management Systems – Requirements, 2005
ISO/IEC, Standard 27002: Information Technology - Security techniques. Code of practice for information security management, 2007
ISO/IEC, Standard 27005: Information Technology - Security techniques - Information security risk management, 2008
Mäkinen, Heikki: Yhteiskunnan tiedon turvallisuus, Versio 2.0, yhteiskunnantieto.fi, 2008
Mäkinen, Heikki: The Social Foundations of Information Security, 2009, White Papers 10, yhteiskunnantieto.fi
Mäkinen, Heikki: The Social Foundations of Information Society Services, 2009, White Papers 11, yhteiskunnantieto.fi
Mäkinen, Heikki: Information Society Services and the Change of Social Rationality, 2008, White Papers 12, yhteiskunnantieto.fi
Mäkinen, Heikki: Global, History and Social, 2008, White Papers 13, yhteiskunnantieto.fi
Mäkinen, Heikki: Knowledge Relation and Social Rationality, 2009, White Papers 14, yhteiskunnantieto.fi