

Risk Management System Development

Risk Management

Social relationships are developing in management of global risks (Mäkinen, 2008, Mäkinen, 2008/13, Mäkinen, 2009/14). This specifies information security management system where are implemented the measures risk management requires. Information security risk management system constitutes of identification and specification the threats directed to social relation. This requires specification of probability and consequences of risks. For risk management are planned and implemented measures according to which information security management is developed.

Risk management principles are same regardless are risks assessed physical, economic or information security risks. Information security management differs from other forms of risk management because there is managed the principal relationship in social, Knowledge Relation (Mäkinen, 2008, Mäkinen, 2009/10, Mäkinen, 2009/14).

Risk management system treats systematically risks activity encounters. It is specified for organization and information society service.

strategy. Risk assessment is a formal process. It aims at to define risk level, risk profile and principles for decision making on risk treatment (ISO 27005, Mäkinen, 2008).

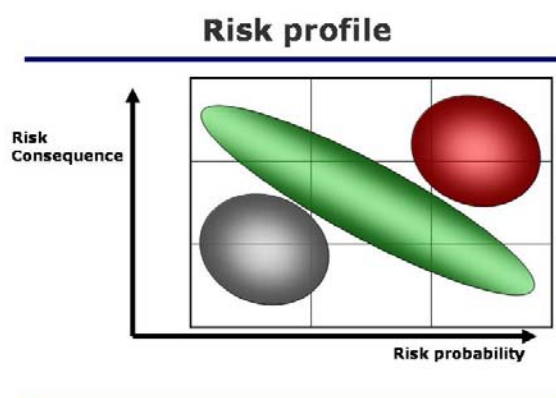
Risk Evaluation

Risks are described as a risk profile by consequences and probabilities (Mäkinen, 2008). Risk profile describes risk level as a whole regarding the objectives of the activity. Risks concerning single factors in division of labour and their management on foundation of instrumental selection are possible to specify in knowledge relation based on conceptual knowledge regarding social structures. In general case, as in information society services, management is developed on foundation of objectives based on information security social relation. For presentation of risk profile there must exist a method.

By risk profile risks are made commensurable. Risk assessment and measurement results must be comparable and repeatable in order that the development of risk level can be controlled. Information security risks are not measurable exactly. Their assessment is based on classification of probability and consequences of risk's



Foundations of risk management are risk criteria, risk scales for evaluation of risks, acceptable risk level and priorities of risk assessment, all defined according to



order of magnitude. On ground of this classification is specified what kind of measures should be directed to each class of risks.

Identified risks are for purpose of evaluation classified according to consequences and probability. Risk profile is assessed on ground of risk distribution; they should follow normal distribution. This is realized if they are situated on a diagonal (green colour): then risk management activities are in equilibrium with identified threats from the point of view of objectives and costs. Risk taken is acceptable.

If risks are situated to area of insignificant consequences and low probability (grey colour), risk management has probably been oversized compared with requirements: to risk management has been invested more than acceptable risk level has presupposed. If risks are emphasized to area of significant consequences and big probability (red colour), situation is not in equilibrium: risk management activities are insufficient.

Risk profile defines level for evaluation of risks. When risk assessment is repeated regularly by commensurable principles, it is possible to estimate and measure risk level and its development.

Ongoing Risk Management

By risk management information security management system is adjusted to changing global threats. This presupposes the continual follow up of risks (ISO 27005).



For ongoing risk management should be defined a formal process. It includes monitoring, reporting of identified risks to

management and decision making for corrective actions in risk management.

Premise for ongoing risk management is strategic objectives according to which are made decisions for risk treatment. On ground of objectives is assessed how effectively risk management has functioned.

Definition of acceptable risk is premise for risk management and information security. This risk level is starting point for risk management planning. In risk reporting is presented how specified risk level has been achieved. Residual risk - risk remaining after risk treatment - should be smaller or equal than accepted risk.

On ground of former topics should be defined what kind of corrections should be made in risk management.

Risk Management Development

Risk management development consist of

- Planning of risk management system as a management and information security management system
- Specification of risk assessment process at level organisation or information society service requires.

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: Global, History and Social, 2008, White Papers 13, yhteiskunnantieto.fi
Mäkinen, Heikki: Knowledge Relation and Social Rationality, 2009, White Papers 14, yhteiskunnantieto.fi