FOURLIS
ΟΜΙΛΟΣ ΕΤΑΙΡΙΩΝ

FOURLIS Group Information Security Risk Management Methodology

This document provides guidelines for FOURLIS Group of Companies Information Security risk Management Methodology and it briefly describes the relative process and its activities.

A systematic approach to information security risk management is necessary for FOURLIS Group of Companies to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS).

Our security efforts address risks in an effective and timely manner where and when they are needed. Information security risk management is an integral part of all our Information security management activities and it is applied both to the implementation and the ongoing operation of the ISMS. The process establishes the external and internal context, assess the risks and treats the risks using a risk treatment plan to implement the recommendations and decisions.

Risk management analyses what can happen and what the possible consequences can be for our Group of Companies, before deciding what should be done and when, to reduce the risk to an acceptable level. Information security risk management contributes to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Personnel being educated about the risks and the actions taken to mitigate them.

An appropriate risk management approach has been selected which is COSO ERM addressing basic criteria such as risk evaluation criteria, impact criteria and risk acceptance criteria.

Risk evaluation criteria are developed for evaluating our organization's information security risk, considering the following:

- The strategic value of the business information process

- The criticality of the information assets involved
- Operational and business importance of availability, confidentiality and integrity
- Stakeholders' expectations and perceptions, and negative consequences for goodwill and reputation

Additionally, risk evaluation criteria can be used to specify priorities for risk treatment.

Consequently, impact criteria are developed and specified in terms of the degree of damage or costs to our organization caused by an information security event considering the following:

- Level of classification of the impacted information asset
- Breaches of information security (e.g. loss of confidentiality, integrity and availability)
- Loss of business and financial value
- Impaired operations (internal or third parties)
- Disruption of plans and deadlines
- Damage of reputation

Risk acceptance criteria depend on our organization's policies, business goals, objectives and the interests of stakeholders. Risk acceptance criteria are set up considering business criteria, our Group Companies operations, the available technology, Finance, social and humanitarian factors.

The threats that are being evaluated and monitored based our Group Information Security Risk Assessment Methodology are:

Physical damage such as fire and water damage

Natural events such as Meteorological phenomenon and seismic phenomenon

Loss of essential services such as failure of air-conditioning or water supply system and failure of telecommunication equipment

Compromise of information such as remote spying, theft of media or documents, theft of equipment, tampering with hardware and tampering with software

Technical failures such as equipment failure and software malfunction

Unauthorized actions such as unauthorized use of equipment and corruption of data.

Compromise of functions such as error in use and abuse of rights.