

2). Risk Management:

The Risk Management is applied in order to evaluate and analyse security risks and threats, and to ensure the implementation of the best security practices to fit Data Compliance rules and laws as well as to allow the correct implementation of data protection.

Different strategies can be used to identify and assess risks as can be the performing of periodic penetration tests, the continuous monitoring of the network resources and communications and the implementation of Intrusion Detection systems through threat alerts.

The evaluation of security policies implemented by other organisations in the past, also called benchmarking, it is also a valuable method for Risk analyse and management implementation.

An essential part of Risk Management procedure is the implementation of Contingency Plans to ensure disaster recovery, and Business Continuity and effective timely response periods when addressing security breaches.

This can be achieved by the application of various elements as employee training and awareness (SETA) to ensure that the members of an organisation are ready to deal with security threats and to implement good practices to prevent from security failures.