mediaservice.net
CORPORATE SECURITY & IMAGE

IT Risk Management

In compliance with the ISO/IEC 27005:2008 standard

What is Risk Management?

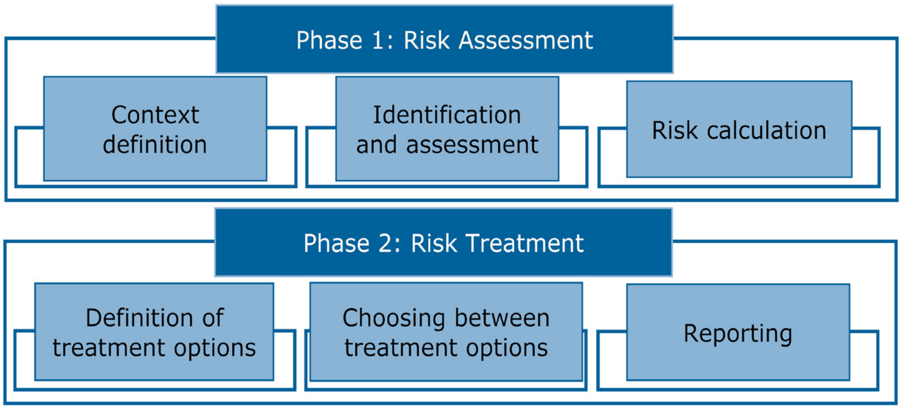
Risk Management is a process that, as a first step, increases risk awareness and afterwards manages the risks to which the company's assets are exposed. This process, within the IT environment, allows for the definition of guidelines aimed at reducing the risks and improving the company's security posture.

The main components of this service are the Risk Assessment and the Risk Treatment activities.

@ Mediaservice.net's offer

@ Mediaservice.net has accumulated a long experience in the field of technological and organizational security, devoting particular attention to training aimed at obtaining specific, field-related skills in Risk Management.

The offered services cover a wide range of needs and are mostly oriented to provide a snapshot of the current risk level and to reduce it. The security requirements based on national and international laws are covered, in compliance with recognized regulations and best practices.



Phase 1: Risk Assessment

Context definition | Identification and assessment | Risk calculation

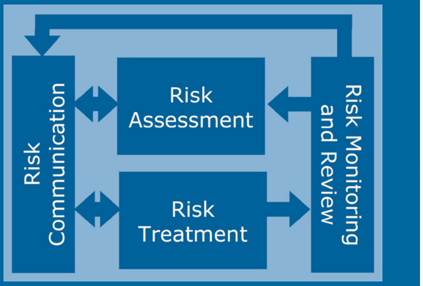
Phase 2: Risk Treatment

Definition of treatment options | Choosing between treatment options | Reporting

The main phases of the service are:
Risk Assessment: the first phase, which includes the definition of the scope, the evaluation of the key parameters (such as assets, vulnerabilities, threats, impacts, and countermeasures), and, finally, the estimation of the residual risk.
Risk Treatment: if the detected risk level exceeds the acceptable threshold, a set of activities is defined, evaluated, and implemented in order to reduce the risk level to the agreed limits.
The results can be expressed qualitatively or quantitatively.

ISO/IEC 27005:2008

This standard defines the guidelines for Information Security Risk Management, in compliance with the ISMS requirements specified by the ISO/IEC 27001:2005.



Compliance with Italian legislation

- Legislative Decree 196 of 2003 "Privacy law".
- Legislative Decree 231 of 2001 "Administrative responsibility".
- Law 262 of 2005 "Law on public savings and regulation of financial markets".

Compliance with foreign legislation

Sarbanes-Oxley Act, Public Company Accounting Reform and Investor Protection Act of 2002.

Compliance with regulations

The Risk Management process is a requirement specified by various international regulations, among which:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- COBITv5
- ISO/IEC 20000-1:2005
- PCI-DSSv2
- Basilea 3
- ISO 22301:2012

Tools and methodologies

@ Mediaservice.net makes use of risk analysis methodologies internationally recognized.

Upon request, @ Mediaservice.net's staff can develop and use proprietary methodologies and tools, in order to align the Risk Management service to the specific needs of the Client.

Optional services

@ Mediaservice.net recommends, as an opportunity to optimize and broaden the relevance of the results provided by the described service, the following additional options:

- *IT Risk Management* Training - theoretical courses and practical coaching of the personnel in charge of IT Risk Management in order to enable it to autonomously carry out a broad range of activities;
- *Internal methodology definition* - creation of an internal methodology for the Client's specific environment, formally establishing criteria, restrictions, roles and responsibilities, execution modes, and guidelines to be followed internally.
- *Quantitative method* - a financial evaluation is added to the risk management activities in order to allow for an universal and objective risk assessment, together with a cost-benefit analysis of the countermeasures taken to mitigate it.

References and Partnerships

@ Mediaservice.net, thanks to its ten-year experience in the security field, can support the realization of any project in an unique way, based on internationally recognized standards and methodologies, such as:

- ISO/IEC 27001
- OSSTMM
- OWASP
- ITIL
- COBIT

Furthermore @ Mediaservice.net boasts the knowledge acquired through strategic partnerships with national and international professional associations and expertise centers

Market sectors

@ Mediaservice.net successfully provides its consulting services to various market sectors. The following real examples of in-field experiences have been anonymized:

Finance	Credit and debit card security assessment for national banks
Transportation	Information security assessment and risk treatment for an airline company
Services & Commerce	Security assessment and risk treatment for the national critical infrastructure (energy sector)
IT Services	Risk assessment and management for national service providers