mediaservice.net
CORPORATE SECURITY & IMAGE

Security Audit

In compliance with the ISO/IEC 27005:2008 and OSSTMM standards

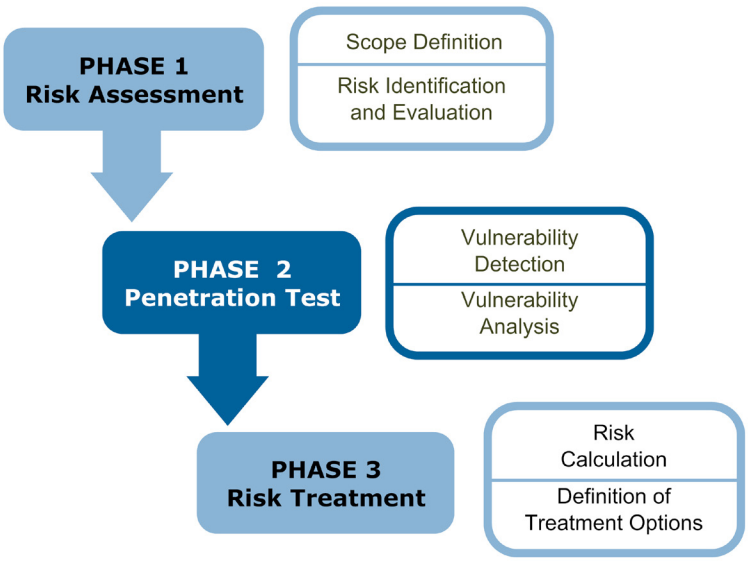
What is a Security Audit?

The Security Audit represents an innovation in the field of IT risk management. It combines the **Penetration Test** and the **Risk Assessment** activities in one, unique service.

The result of this synergy is an extremely detailed analysis, that is aimed at precisely assessing the security posture of the Client's IT infrastructure. The analysis is supported by technological evidence, in compliance with formal assessment methodologies.

@ Mediaservice.net's offer

@ Mediaservice.net has accumulated a long experience in the field of technological and organizational security and has acquired the wide range of skills required to identify and evaluate risks in different scenarios. In order to provide a complete security management framework it is mandatory to correlate information related to both technological and organizational aspects. The following diagram describes the phases of a Security Audit activity (the sections colored in light blue are related to organizational security, while the ones in dark blue refer to technological security):



The distinguishing property of the Security Audit is the combined use of two types of assessments that allows:

- optimization of the Penetration Test activity, by increasing its efficiency and providing the best possible vulnerability evaluation;
- improvement of the precision of risk detection and of mitigation strategies, by including an additional layer of technical detail.

ISO/IEC 27001:2005

This standard defines a PDCA (Plan-Do-Check-Act) cyclic process for the Information Security Governance. The main areas that are covered by the regulation are:

- Security policies
- Organization
- Asset management
- Personnel training
- Physical security
- Security of operations and communications
- Access control
- Development process security
- Incident handling and continuity management
- Compliance

OSSTMM

The "Open Source Security Testing Methodology Manual" is an open methodology for executing IT security tests and measuring their results. It is organized in five channels that allow for complete test coverage: TLC, Data networks, Wireless, Physical Access, and Personnel.

When to perform a SA

1. As a first step for a perimeter that has never been analyzed before
2. For the evaluation of processes that pose life-threatening risks
3. For the evaluation of critical infrastructures and systems
4. For the evaluation of financial transactions
5. For a comprehensive Risk Assessment in compliance with ISO/IEC 27001 or PCI-DSS standards

Tools and methodologies

For the **Risk Assessment** component of the service, methodologies compliant to the ISO/IEC 27001:2005 and ISO/IEC 27005:2008 standards will be used. Both qualitative and quantitative (in euros) risk assessments can be carried out.

For the **Penetration Test** component, the OSSTMM is used. For ten years, this methodology has been a reference point in the field and it is widely supported nationally and internationally. It covers five channels (TLC, Data networks, Wireless, Physical Access, and Personnel), that are analyzed according to the detected security needs.

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;
- *Penetration Testing Training* - theoretical courses and practical coaching of the personnel in charge of the technological assessments in order to enable it to carry out such activities autonomously;
- *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;
- *Follow-up* - verification of the correct implementation of the security countermeasures suggested within the remediation plan.

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	Information security assessment and risk treatment for a medium-sized bank
Transportation	Information security assessment and risk treatment for an airline company
Services	Security assessment and risk treatment for the national critical infrastructure (energy sector)
Luxury and Fashion	Information security assessment and risk treatment for a leading luxury company

mediaservice.net
CORPORATE SECURITY & IMAGE

@ Mediaservice.net S.r.l.
Via Santorelli, 15 - 10095 Grugliasco (TO)
Tel +39 011-3272100 - Fax +39 011-3246497
info@mediaservice.net - **www.mediaservice.net**