mediaservice.net
CORPORATE SECURITY & IMAGE

Gap Analysis and IT Audit

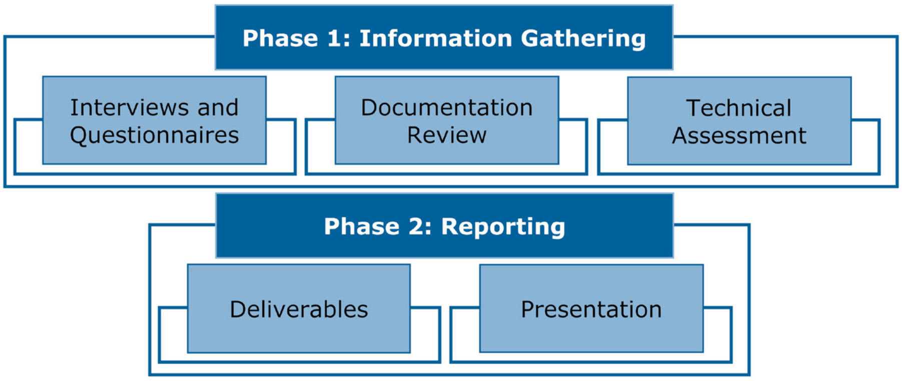
What are Gap Analysis and IT Audit?

A **Gap Analysis** is an activity aimed at identifying the gap between the actual security posture and a regulation, a law or any set of requirements, by a thorough examination. The output of the analysis is a precise description of the missing elements that are necessary to fill the identified gap.

An **IT Audit** is a formal process aimed at assessing the compliance with a regulation, a law or a company's policy. This activity is carried out on a selected sample of assets, following the ISO 19011:2012 guidelines and ISACA standards, in order to provide compliance and non-compliance results supported by evidence collected in the field. It can be performed internally (first party audit) or on behalf of an external purchasing entity (second party audit).

@ Mediaservice.net's offer

Following its approach and methodology developed internally and backed by years of experience, @ Mediaservice.net organizes the Gap Analysis and IT Audit activities in the following operational phases:



In detail, the first phase (**Information Gathering**) is based on risk parameters and is aimed at matching the IT processes with the required control objectives. The methodology for gathering the needed data differs depending on the environment and on the identified requirements.
During the second phase (**Reporting**), the collected evidence is analyzed and formally organized, in order to be reported together with the detailed remediation advice.

ISO/IEC 27001:2005

This standard defines a PDCA (Plan-Do-Check-Act) cyclic process for 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

Privacy

The Legislative Decree 196 of 2003 and the related measures define the minimum requirements for handling and protecting sensitive personal data.

COBIT 4.1

This regulation establishes a series of processes and control objectives for IT management, organized in the following categories:

- Plan and Organize (PO), concerning high-level processes for management and governance
- Acquire and Implement (AI), related to IT systems deployment processes
- Deliver and Support (DS), concerning provisioning and operational management
- Monitor and Evaluate (ME), related to control and compliance with internal and external regulations

Available audit criteria

@ Mediaservice.net's professional resources have accumulated a solid experience, proven by LA27001, CISA, and ITIL accreditations. The Gap Analysis and IT Audit services are usually performed in accordance to the following criteria:

- ISO/IEC 27001:2005;
- Privacy (Legislative Decree 196/2003);
- Computer crime (Legislative Decree 231/2001);
- ISO/IEC 20000-1:2005;
- PCI-DSSv2;
- ISO 22301
- BS 25777:2008;

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:

- *Definition of treatment plans* – support in the design, deployment, and monitoring of remediation tasks, in order to fix the detected non-compliances;
- *Risk Assessment* – extended activity aimed at considering information security risks associated to the detected non-compliances, in order to correctly prioritize the remediation tasks;
- *Internal methodology definition* – support in creating an internal methodology and defining a structured and complete audit plan, as required by most international regulations.

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	Multiple ISO/IEC 27001 first party audits
Transportation	Documentation audit for a national regulatory body
Services	ISO/IEC 27001 first party audit for a software house

@ 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**