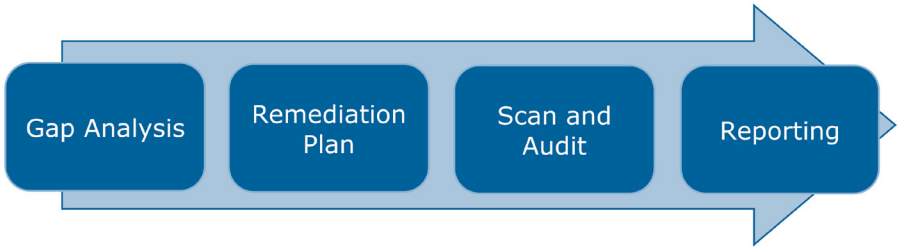
mediaservice.net
CORPORATE SECURITY & IMAGE

PCI-DSS Compliance

What is PCI-DSS?

PCI-DSS is the acronym of Payment Card Industry – Data Security Standard. It is an international regulation created by the main payment brands in order to reduce the security risks faced by merchants, service providers, and final customers in the credit card sector.
The standard details a number of security requirements that must be applied to environments where payment card data are processed, in order to reduce the attack surface and mitigate the impact of potential security incidents.
PCI-DSS is compliant with the security best practices relevant to the specific sector.

@ Mediaservice.net's offer



Thanks to its ten-year experience in the security field, @ Mediaservice.net has developed a complete offer aimed at supporting its Clients in any phase of the PCI-DSS certification process. The consulting service starts with a **Gap Analysis**, aimed at examining card data flows and assessing compliance with the requirements specified by the regulation, also through technological security tests.
After such analysis, a detailed **Remediation Plan** is produced outlining the specific actions needed in order to reach a fully compliant state. These actions can be carried out internally or with the support of @ Mediaservice.net's specialists (see optional services below).
The next step is carrying out the actual **Audit and Security Scan** activities, based on internationally recognized methodologies in order to validate the execution of the Remediation Plan.
Finally, within the **Reporting** phase the official deliverables needed for the statement of compliance are produced.
These last two activities can be purchased separately and must be periodically repeated in order to maintain the certification

Who should be compliant to PCI-DSS?

The regulation affects any organization that processes payment cards, such as:

- Merchants
- Banks (Issuers and Acquirers)
- Service Providers

The requirements must be fully applied regardless of the size of the specific entity.

PCI-DSS requirements

- Deploy and maintain a secure network
- Protect payment card data
- Follow a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test the IT infrastructure
- Implement a Security Policy

The creators of the PCI-DSS regulation

The PCI-SSC (Security Standards Council) encompasses the following brands:

- VISA, Inc.
- Mastercard Worldwide
- JCB International
- American Express
- Discover Financial Services

Added value

- Mitigation of risks related to processing payment card data
- Reduction of costs associated with security incidents
- Improvement of the security posture as perceived by customers and partners
- Compliance with compulsory requirements, in order to avoid fines

Operational references

@ Mediaservice.net's consulting services are based on the latest release of the PCI-DSS regulation (now at version 2) and related documents, on the ISO/IEC 27000 family of standards, and on the OSSTMM and OWASP open methodologies, that are particularly significant for providing an added value.

Optional services

Besides the activities described above, @ Mediaservice.net recommends, as an opportunity to optimize and broaden the relevance of the provided results or support the Client in the execution of the Remediation Plan, the following additional options:

- drafting or review of required plans, policies, and procedures;
- execution or review of the Risk Assessment;
- execution of technological security assessments (e.g. Penetration Test, Wireless Scan) or IT Audits, also outside of the scope defined by PCI-DSS;
- execution of in-depth technological assessments where needed (e.g. source code review);
- support of the IT staff in planning and implementing the technical countermeasures outlined in the Remediation Plan;
- training of Client's professional resources;
- integration of the PCI-DSS compliance requirements within a broader ISMS compliant with the ISO/IEC 27001:2005 standard.

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	Support in reaching PCI-DSS compliance for national banks.
IT Services	Support in reaching PCI-DSS compliance for service providers.
Online Shopping	Support in reaching PCI-DSS compliance for online shops.
Tourism	Support in reaching PCI-DSS compliance for tour operators.

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**