

PCIDSS

Anyone accepting card payments either on-line or by telephone needs to comply with the PCIDSS security standard. The standard covers electronic and hard records, data at rest and in transit. There are tough penalties for failing to demonstrate compliance. Acenseo have a demonstrable track record in helping clients meet PCIDSS compliance without making unnecessary financial or resource investments.

How can you achieve compliance with remediation that takes into account real business decisions; instead of wasting time and resources on “book driven” remedies?

Acenseo provides a fully compliant security test of on-line resources which can be carried out on demand throughout the contract term. This means that you can quickly recheck after any upgrade or change to hardware, software or web pages. This process allows for easy visibility of pass level and one step online submission of both test and questionnaire sections for compliance.

In addition Acenseo provides assistance with remediation and corrective action plans to ensure compliance. Our consultants have a thorough understanding of both threats and business drivers to ensure that solutions are both economical and complete. As a 24x7x365 organisation remediation can be carried out outside of your core hours and in line with change control policy to eliminate unnecessary downtime.

Acenseo can also assist with digital patching of systems by preventing vulnerabilities from being successful, mitigating denial attacks and content checking for account data in transit. The resulting solutions ensure legacy systems can be compliant without onerous workloads or rewrites.

Simplify the PCIDSS compliance process and ensure assistance from a trusted security advisor, allowing for the business needs to be met, and using this opportunity to ensure your infrastructure and procedures are less prone to data loss.

The PCIDSS service is part of the Ascend CONSULT offering. Additional Ascend services include Ascend ID, Ascend TRAIN, Ascend SUPPORT and Ascend MANAGE.



IT Healthcheck

Modern IT networks offer multiple entry points, and consequently exit points, for data communication. User access demands often permit desktop access from insecure third party networks, whilst WIFI connections allow eaves dropping from a distance. Keeping on top of these evolving challenges requires thorough testing to identify possible weak points, and experienced corrective planning to avoid restricting user access, to the detriment of the business.

Acenseo provides a comprehensive IT Health Check service. This holistic service incorporates external, internal and wifi access methods, comprehensive reporting, analysis and an onsite debrief. Adopting the widely respected OSSTMM methodology, the CHECK standard and also using ethical hacking techniques that do not store or change your sensitive data, Acenseo's testing does not store or change any client sensitive data ensuring the integrity of the information. Furthermore, our approach is such that we ask for permission from our clients to access their results, which can be deleted upon request at any time.

External testing consists of thorough information gathering, including access to your systems as well as cached details via third parties. This is followed by a scan of internet assets and applications which we intelligently identify and test to. We then repeat and validate our findings to identify true risk, so apparent weaknesses which are mitigated via other policies are accurately assessed. Finally, we use post testing procedures to mimic how far a real intruder could enter your systems. All services are provided outside of office hours to ensure minimal impact on business systems.

The internal testing procedure consists of intelligently assessing the scope of your network resources, and identifying critical network, server and workstation devices for testing. Acenseo perform a comprehensive network penetration test to gain access to resources, identify compromised systems & detect vulnerabilities. We then analyse the results, and if vulnerabilities are exploitable, we attempt access/privilege escalation techniques to validate the true security posture of the network.

WIFI testing techniques differ from wired in that we test for RF weaknesses as well as gaining access and eavesdropping. This is achieved by identifying rogue access points, and denial of access to wireless access points.

Web application testing utilises automated and manual code reading techniques to identify weaknesses, denial attacks and data leakage methods. This includes the OWASP Top Ten web application weaknesses:

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

The IT Healthcheck is included within the Ascend CONSULT offering, and is part of the Ascend services portfolio which includes Ascend ID, Ascend TRAIN, Ascend SUPPORT and Ascend MANAGE.



ISO 9001 - A certified quality management system promotes, facilitates and enables consistency and improvements in a process or product.



ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS).

Acenseo Ltd

Tel: +44 (0)1189-790000
Fax: +44 (0)1189-406327

Acenseo Ltd, Hare Hatch Grange, Bath Road, Hare Hatch, Berkshire, RG10 9SA

Copyright: ©2010 Acenseo



acenseo
secure systems integration

www.acenseo.com