



PCI DSS

Cutting PCI Compliance Down To Size

You can achieve PCI compliance.
Ambersail provide all the answers.

- ✓ Complete PCI audit solution - QSA and ASV
- ✓ International customer base
- ✓ Cost effective, fixed price services
- ✓ Helpful, practical and informative approach
- ✓ Independent, vendor neutral

Cutting PCI Compliance Down To Size

Ten PCI Compliance Tips

As an established PCI Auditor, Ambersail has delivered independent compliance services to a wide range of organisations.

During our investigations, we find our clients are confronted with a range of similar issues. These include:

1. Understanding where your cardholder data is

When it comes to becoming PCI compliant, you need to be able to demonstrate that you know:

- where cardholder data enters and leaves your network (e.g. web sites, call centres, post orders),
- how cardholder data is processed (e.g. how applications process data, how receipts are processed, how orders are reconciled),
- where cardholder data is stored (e.g. ecommerce databases, spreadsheets, management reports).

Knowing where data is stored, processed or transmitted is the first step towards scoping your compliance programme. Remember, PCI audits only review ring fenced card processing networks.

A vast amount of compliance effort can be saved by removing redundant card data.

2. Avoid bespoke cryptography

When developers review PCI data storage requirements, many will never have fully employed encryption before. There is a tendency to try and reinvent the wheel and write their own encryption algorithm to protect cardholder data. PCI-DSS does not recognise these home-grown algorithms.

Do not re-invent cryptographic tools. Use proven standards such as RSA or AES.

3. Instances of debugging logs

It is common for developers to produce detailed logs from within applications that process card data. If unchecked, logging facilities can migrate into the live environment - printing execution progress out to a log file for debugging. The problem comes when these logs also contain cardholder data.

When looking for cardholder data, your PCI Auditor will pay close attention to any logs produced by your applications.

4. Wireless Network Separation

While PCI usually considers "in-scope" equipment and wired networks, wireless networks are the exception. If you have a wireless network on the same network used to access cardholder data, then this wireless network needs to be protected with strong encryption - as well as a firewall.

All wireless networks need to be firewalled if they have access to another network that stores, processes or transmits cardholder data.

5. Third parties, payment applications and service providers

Outsourcing the management of infrastructure may make many aspects of PCI easier. However you need to ensure that contracts are in place between yourselves and any third party that ensures they manage your card data in a compliant fashion. Where a third party company can access cardholder data then this company is a Service Provider under the terms of PCI and must be PCI compliant too.

Ensure that contracts also allow access to any affected servers in case of a breach, both by you and any forensic auditors that may be required.

Third party payment applications may also bring their own non-compliance issues. The Payment Application Best Practice standard exists to ensure that software providers can offer solutions that will not prevent you from validating your own compliance. Note that from 1st January 2008, Visa US is starting the enforcement of PABP in order to eliminate non compliant payment applications.

Outsourcing does not exclude you from compliance validation. Where an on-site audit is required, your PCI Auditor may need to review your service provider's card processing arrangements too. Also bear in mind that non-compliant third party payment applications may prevent you from becoming compliant.



6. Policies

Much of PCI DSS section 12 is devoted to company policies, from information security policies to disaster recovery. Many of these policies require annual examination and walkthroughs to ensure they are kept current. By the time your PCI audit comes around, your company should be adhering to all the rules of the DSS – and you need to be able to prove it.

Where you are undergoing an on-site audit, expect your policy documents to be inspected, and your staff queried as to their understanding of those policies.

7. Scoping & Network Segmentation

To accurately scope your cardholder network, you need to fully understand where your cardholder data is stored, transmitted or processed.

Identify machines that are on the same network – but do not handle cardholder data – and establish whether these servers even need to be there.

It is common to find card data held in arbitrary files – possibly for reconciliation or accounting purposes. These files constitute data stores and, as such, will render the networks that host them in scope for PCI auditing.

Now is a good time to make sure that your systems documentation is up to date. Make early decisions about isolating card processing systems, which will reduce audit scope.

8. Organisational Boundaries

The PCI-DSS spans the entire card processing environment. This means that managers from networking, ecommerce, personnel and call centres all have a contribution to make.

You are a stakeholder. Don't assume that PCI compliance is just an IT issue.

9. Making The Best Use Of Your Auditor

Your QSA or ASV should help you to become PCI compliant as quickly as possible. For larger Merchants and Service Providers where an on-site audit is required, missing out details at the gap report that are later discovered at the final audit, may force you to re-start the audit process where remediation cannot be implemented within 30 days of the final audit taking place.

Confronting the PCI compliance issue with straightforward, honest answers will enable your PCI Auditor to guide you towards compliance as quickly as possible.

10. Web Application Security

Requirement 6 of the DSS places great importance on understanding and managing web vulnerabilities. Unfortunately many organisations do not consider web vulnerabilities to be an issue for web developers – a significant fact considering that much stolen card data emanates from vulnerable web applications.

Your software development lifecycle must now include standards for secure coding & testing such as those found at www.owasp.org

Contacts and Additional Information

If you wish to learn more about Ambersail's capabilities, please don't hesitate to call us on **0870 011 8163** or visit the website on **www.ambersail.com**

About Ambersail

Ambersail is a UK based security audit consultancy that serves EU and CEMEA region clients. We specialise in providing protection and guidance on the security of online applications, supporting infrastructure and brand assets.

We believe that a PCI Auditor should be a trusted advocate for a client. This trust is built as we demonstrate our deep knowledge of how PCI affects every aspect of their card processing operations.

Our independent audit team is built from the brightest minds in payment processing and technology consulting and will actively seek to reduce the time spent to reach your PCI compliance objective.

Why choose us...

- We are an established PCI auditor. We have been performing audits for Merchants and Service Providers for several years and have helped many organisations achieve compliance. We have extensive experience in working with our clients to complete official audit documents and remediation tasks.
- Our goal is to get PCI audit clients compliant as quickly and painlessly as possible.
- We offer a comprehensive PCI service that includes onsite QSA audits, PABP reviews, external ASV scans and mandatory PCI exercises such as penetration testing and strategy review. All of these services are provided directly by Ambersail, not via third parties. This enables us to set prices at a very competitive level.
- Our technical audit solution has been developed in house. Approved by the PCI Standards Council, it is currently used by many notable organisations across the world – including both PCI and non-PCI organisations.
- We value a personal approach when working with our audit clients. This extends to offering ad-hoc advice and fielding questions from customers at no extra cost. We take time and effort to liaise with the various PCI standards bodies to ensure that our clients get the very best advice.

Contact:

Jon Morris
Ambersail, Walton Lodge, Hill Cliffe Road, Warrington.
WA4 6NU. United Kingdom.

Telephone: + 44 (0) 1925 600062
Email: jon.morris@ambersail.com