

What should I do about PCI Compliance?

1. If I have not yet started with my PCI work, what should I do right now?
 - Start identifying all the systems that touch cardholder data, because all of these systems will be in scope for your eventual PCI DSS Compliance Validation. The Payment Card Industry Data Security Standard (PCI DSS) is focused on how you treat “cardholder data”, such as account numbers. A big part of any PCI assessment is determining where cardholder data is processed, transmitted, or stored. You may be surprised to find out the number of system retaining cardholder data, including data warehouses, staging servers, middleware, backup systems, etc.
 - Your IT team needs to be familiar with the PCI Data Security Standard. Make sure you are using the latest version – you can find it at https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm. Note: Version 1.1 released in September 2006 included updates that made the standards much easier to understand.
 - Contact your software and hardware vendors. Find out if the versions of their products that you are using have passed PCI DSS compliance validation. There is a list of validated payment applications on the Visa web site.
 - Contact your card processing and network service providers. If you are using third party managed services, then the same question should be asked of them – has your service passed PCI DSS compliance validation. The Visa web site also has a current list of PCI complaint service providers.
 - If your company operates its own network, then your network team needs to start reviewing the PCI Data Security Standard. Many of the 12 key requirements are directly related to network components. Several are common sense, for example do not use vendor default passwords.
 - Get your testing team involved. Their test procedures will be checked as part of a PCI DSS compliance validation.
 - Take advantage of whatever security measures you already have in place. Much of the PCI Data Security Standard is based on good system management practices. If your current data security standards are in good shape, you may be able to meet some of the PCI requirements by just updating your existing policies.
 - Once your team is familiar with the PCI requirements, conduct a candid internal assessment. Decide where you think you are related to each of these requirements. Begin making the obvious changes right away.
 - Consider hiring a consultant very familiar with the whole PCI assessment and validation process.

2. How can I reduce the amount of work I have to do to be PCI compliant?
 - PCI Data Security Standards (PCI DSS) requirements must be met for any system that stores, processes, or transmits cardholder data. Processing and transmitting account numbers is essential in any system that authorizes card transactions. However, retailers in the past have often stored account numbers in additional site and head office systems so they can look up the transaction

later if it is disputed. There are other ways of finding a specific transaction: reference number is often the easiest. If you reduce the number of systems that touch cardholder data, then you reduce the scope of your PCI compliance validation efforts.

- Get your key vendors involved. Ask them if their products are PCI DSS compliant. If so, are there any version upgrades or configuration options you need in order to make sure your systems can pass the PCI DSS Compliance Validation? If their products are not PCI DSS compliant, then what are their plans for addressing PCI DSS compliance, and when will they deliver a version that has been PCI DSS validated?
- Make PCI DSS compliance part of the criteria for any new retail system selection. This is not your problem; it is the whole industry's problem. It is reasonable to expect all new vendors to deliver software, hardware, and network components that are PCI compliant.
- Separate your networks that handle card data from other site and head office networks. If you provide Internet access for your site manager, there needs to be a firewall between your card network and the network handling Internet traffic. This does not necessarily mean multiple network connections on site – there are network providers that will provide a single physical connection that separates the two types of traffic.

Summary of the 12 PCI Requirements

Securing and Protecting Cardholder Information is the main role of the PCI (Payment Card Industry) Security Standards Council.

The PCI Security Standards Council was founded in September, 2006 by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. It is “an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.” -- This is from the PCI Security Standards Council web page:

<https://www.pcisecuritystandards.org/> Membership on the council is open to issuers, merchants and vendors.

The PCI Data Security Standard (DSS) is a list of 12 requirements organized in 6 areas/objectives. These security standards apply to all system components that store, process or transmit cardholder data.

A. Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Key Message

Properly segment your network, and protect network segments that store, process or transmit cardholder data. This includes not only the network segments from an enterprise level – but at each retail site. To properly segment and protect the network segments, firewalls must be implemented. The firewall rule set should have a business rule for every service, port and action configured.

B. Protect Cardholder

3. Data Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Key Message

Never store Track data (Mag Stripe), Security Code (CVC2/CVV2/CID) or PIN/PIN Block after authorization. Minimize storage of other card related data. The PAN (Primary Account Number) can be stored for business reasons if encrypted properly. Cardholder data must be encrypted when transmitted across public networks. Under PCI, Wireless networks are treated as public networks and must have appropriate encryption transmission and firewalled segmentation.

C. Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Key Message

Execute effective security practices on all applications and infrastructure. Assign someone the explicit responsibility for keeping security patches and anti-virus capability up to date on all computers – headquarters and at site.

D. Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Key Message

Ensure support access is configured appropriately with appropriate logging. This must be established and reviewed by POS, back office, 3rd party Help Desk, and any other support providers.

E. Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Key Message

Hire an Approved Scanning Vendor to periodically perform intrusion detection tests on your networks. Ensure appropriate logging of access to all systems processing, storing, or transmitting cardholder data.

F. Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Key Message

Document and share a security policy. It must be viewed as the way of doing business. Develop and maintain an explicit documented security review process that is audited periodically (e.g. quarterly).

Merchants should consider engaging an authorized assessor (Qualified Security Assessor (QSA)) to review and assess the merchant to ensure that they comply with all 12 requirements. A Report on Compliance (ROC) is produced by the auditor. The ROC is provided to the Sponsoring Bank who passes this along to Visa & MasterCard.

Visa has also implemented a Payment Application Best Practice – PABP program. Visa highly recommends that all Payment Applications (including POS and any other equipment processing payments) go through a PABP audit, with an approved auditor, to obtain validation for their application. Visa has a website that lists validated payment applications.



The PABP is basically a subset of the PCI DSS requirements that are specific to a payment application (as opposed to the entire payment network/system components).

Tip: When a merchant is going through their PCI DSS compliance validation, each type of POS used by that merchant will need to be reviewed. If the POS has been through a PABP, the auditor reviews their findings in the merchant's environment. If the POS has not been through a PABP assessment, the auditor will need to in a sense – perform the PABP, on behalf of the merchant, in order to complete the merchant's audit.

Tip: PCI Auditors also highly recommend that all POS devices connected to a merchant's network have been PABP validated. It is believed that the PABP program will roll under the PCI Standards Council and will become a requirement in the near future.

Tip: Key items that are looked at under the PABP relate to Protecting Cardholder Data and Implementing strong access control measures. Additionally, the application must work appropriately in a secure environment.

Thank you to the W. Capra Consulting Group for developing this guide for NACS members. W. Capra Consulting Group, Inc. is a consulting company focused on identifying, leading, integrating, and delivering retail and payment technology solutions to convenience, petroleum and retail businesses.