DELL SecureWorks

# PCI Compliance Glossary

The Payment Card Industry Data Security Standard (PCI DSS) has its own vocabulary, which can be daunting if you're not familiar with it. This glossary is designed to help you better understand some of the most common terms and acronyms related to PCI compliance. For a complete list of terms and acronyms, visit the PCI Council website.

| TERM | DEFINITION |
|---|---|
| Acquiring Bank | An acquiring bank is the bank or financial institution that provides accounts to merchants and processes credit and debit card transactions on their behalf. A merchant account allows an organization or company to accept credit cards. The bank or financial institution then deposits the funds into the merchant's checking account. |
| Approved Scanning Vendor (ASV) | An organization approved by the PCI Council to conduct external vulnerability scanning services. |
| Card Brands | Payment card brands, such as Visa, MasterCard, American Express, Discover, and JCB. |
| Cardholder Area | Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment. |
| Compensating Controls | Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. |

## Glossary

| | |
|---|---|
| Compliance Program | Internal program that an organization has developed in order to comply with the PCI-DSS. |
| Configuration | The modifiable settings of a device, application, software, etc. |
| Device | Any IT asset. |
| Dataflow Maps | A type of flow chart; a description of data and the manual and machine processing performed on the data as it moves and changes from one stage to the next. It also includes the locations where the data are placed in permanent storage (disk, tape, etc.). |
| DSS | Data Security Standard. See also PCI-DSS. |
| IP address | An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes. |
| Cardholder Data Environment or In Scope System or PCI Scope Environment | The boundaries and included area in which cardholder data resides. |
| Merchant Levels | Merchant Levels are determined by the annual volume of transactions a business processes, and may vary by card brand. Merchant Levels determine the level of validation and reporting method necessary to demonstrate compliance.  Merchant levels are generally defined as follows: Level 1 - more than 6 million annual transactions; Level 2 - 1 million to 6 million annual transactions; Level 3 - 20,000 to 1 million ecommerce transactions; and Level 4 - fewer than 20,000 annual transactions. Levels are assigned by your acquiring bank, so contact them for confirmation of your PCI Merchant Level. |
| Network Diagrams | A network diagram is a general type of diagram, which represents some kind of network. A network in general is an interconnected group or system, or a fabric or structure of fibrous elements attached to each other at regular intervals, or formally: a graph. |
| Network Segmentation | Network segmentation in computer networking is the act or profession of splitting a computer network into sub- networks, each being a network segment or network layer. The boundary between segments should provide extra security precautions, such as those described in the PCI-DSS. |
| PCI | Payment Card Industry |

## Glossary

| | |
|---|---|
| PCI-DSS | Payment Card Industry Data Security Standard. This is the set of requirements set forth by the PCI-SSC against which compliance is measured. |
| PCI Program | Internal program that Affiliate has developed in order to comply with the PCI-DSS. |
| PCI Security Standards Council (PCI-SSC) | The governing organization and open forum responsible for the development, management, education, and awareness of PCI Security Standards. |
| PCI PFI | PCI Forensic Investigator (PFI). Program set out to create a standardized process for the forensic investigation and reporting of information security incidents involving cardholder information. |
| Qualified Security Assessor (QSA) | The PCI Security Standards Council provides training and certification for professionals performing PCI audits. Organizations should always confirm that their auditor is a certified QSA employed by a QSA Company listed on the PCI SSC website. |
| Technical Testing | Testing in which the consultant interacts with technology. Types of testing may include scanning, configuration validation, etc. |

**For more information, visit http://www.secureworks.com.**

**Email info@secureworks.com or phone 877-838-7947 to speak to a Dell SecureWorks Security Specialist.**