Payment Card Industry (PCI)

Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)

Glossary of Terms, Abbreviations, and Acronyms

Version 1.2

October 2008

Term	Definition
AAA	Acronym for "authentication, authorization, and accounting." Protocol for authenticating a user based on their verifiable identity, authorizing a user based on their user rights, and accounting for a user's consumption of network resources.
Access Control	Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.
Account Number	See *Primary Account Number (PAN).*
Acquirer	Also referred to as "acquiring bank" or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Adware	Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.
AES	Abbreviation for "Advanced Encryption Standard." Block cipher used in symmetric key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or "FIPS 197"). See *Strong Cryptography.*
ANSI	Acronym for "American National Standards Institute." Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
Anti-Virus	Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.
Application	Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides a trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.
Authentication	Process of verifying identity of an individual, device, or process
Authorization	Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction, it is the instance when a merchant receives approved permission for a payment card to be used for a particular transaction.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distance between two devices.
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Term	Definition
Cardholder Data	At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: ▪ Cardholder name ▪ Expiration date ▪ Service Code See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed as part of a payment transaction.
Cardholder Data Environment	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 DSS assessment. A cardholder data environment is comprised of system components. See *System Components.*
Card Verification Code or Value	Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: ▪ **CAV –** Card Authentication Value (JCB payment cards) ▪ **CVC –** Card Validation Code (MasterCard payment cards) ▪ **CVV –** Card Verification Value (Visa and Discover payment cards) ▪ **CSC –** Card Security Code (American Express) (2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following provides an overview: ▪ **CID –** Card Identification Number (American Express and Discover payment cards) ▪ **CAV2 –** Card Authentication Value 2 (JCB payment cards) ▪ **CVC2 –** Card Validation Code 2 (MasterCard payment cards) ▪ **CVV2 –** Card Verification Value 2 (Visa payment cards)
CIS	Acronym for “Center for Internet Security.” Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.
Column-Level Database Encryption	Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see *Disk Encryption* or *File-Level Encryption.*

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 PCI DSS requirement; (2) Provide a similar level of defense as the original PCI DSS requirement; (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. See Compensating Controls Appendices B and C in *PCI DSS Requirements and Security Assessment Procedures* for guidance on the use of compensating controls.
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Console	Screen and keyboard which permits access and control of the server or mainframe computer in a networked environment.
Consumer	Individual purchasing goods, services, or both.
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.
Database	Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.
Database Administrator	Also referred to as "DBA." Individual responsible for managing and administering databases.
Default Accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service.
Default Password	Password on system administration or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Degaussing	Also called "disk degaussing." Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.
Disk Encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (e.g., hard disk, flash drive). Alternatively, *File-Level Encryption* or *Column-Level Database Encryption* is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network or computer host that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct access to devices in the DMZ rather than all of the internal network.

DNS	Acronym for "domain name system" or "domain name server." System that stores information associated with domain names in a distributed database on networks such as the Internet.
DSS	Acronym for "Data Security Standard" and also referred to as "PCI DSS."
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also *Split Knowledge.*)
Dynamic Packet Filtering	See *Stateful Inspection.*
ECC	Acronym for "elliptic curve cryptography." Approach to public-key cryptography based on elliptic curves over finite fields. See *Strong Cryptography.*
Egress Filtering	Method of filtering traffic exiting an internal network via a router such that unauthorized traffic never leaves the internal network.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
Encryption Algorithm	A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again.
File Integrity Monitoring	Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see *Disk Encryption* or *Column-Level Database Encryption.*
FIPS	Acronym for "Federal Information Processing Standards." Standards that are publicly recognized by the U.S. Federal Government; also for use by non-government agencies and contractors.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
FTP	Acronym for "file transfer protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology.

GPRS	Acronym for "General Packet Radio Service." Mobile data service available to users of GSM mobile phones. Recognized for efficient use of limited bandwidth. Particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing.
GSM	Acronym for "Global System for Mobile Communications." Popular standard for mobile phones and networks. Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via *Strong Cryptography*.
Host	Main computer hardware on which computer software is resident.
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.
HTTP	Acronym for "hypertext transfer protocol." Open internet protocol to transfer or convey information on the World Wide Web.
HTTPS	Acronym for "hypertext transfer protocol over secure socket layer." Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins.
ID	Identifier for a particular user or application.
IDS	Acronym for "intrusion detection system." Software or hardware used to identify and alert on network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected.
IETF	Acronym for "Internet Engineering Task Force." Large, open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of Internet. The IETF has no formal membership and is open to any interested individual.
Index Token	A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information Security	Protection of information to insure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Ingress Filtering	Method of filtering traffic entering an internal network via a router such that incoming packets are verified that they are actually coming from the networks they claim to be from.

Insecure Protocol/Service/Port	A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that transmit data and authentication credentials (e.g., password/passphrase in clear-text over the Internet), or that easily allow for exploitation by default or if misconfigured. An example of an insecure protocol, service, or port is FTP.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer on the Internet.
IP Address Spoofing	Attack technique used by a malicious individual to gain unauthorized access to computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.
IPS	Acronym for "intrusion prevention system." Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.
IPSEC	Abbreviation for "Internet Protocol Security." Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer.
ISO	Better known as "International Organization for Standardization." Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland, that coordinates the system.
Issuer	Also referred to as "issuing bank" or "issuing financial institution." Entity that issues payment cards directly to consumers and non-consumers.
Key	In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message. See *Strong Cryptography.*
LAN	Acronym for "local area network." Computer network covering a small area, often a building or group of buildings.
LDAP	Acronym for "lightweight direct access protocol." Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected resources.
LPAR	Abbreviation for "logical partition." A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces.
MAC	Acronym for "message authentication code." In cryptography, it is a small piece of information used to authenticate a message. See *Strong Cryptography.*
MAC Address	Abbreviation for "media access control address." Unique identifying value assigned by manufacturers to network adapters and network interface cards.

Magnetic-Stripe Data	Also referred to as “track data”. Data encoded in the magnetic stripe or chip used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.
Mainframe	Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.
Malicious Software/Malware	Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Masking	Method of concealing a segment of data when displayed. Masking is used when there is no business requirement to view the entire PAN.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
Monitoring	Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
MPLS	Acronym for “multi protocol label switching.” Network or telecommunications mechanism designed for connecting a group of packet-switched networks.
NAT	Acronym for “network address translation.” Known as network masquerading or IP masquerading. Change of an IP address used within one network to a different IP address known within another network.
Network	Two or more computers connected together to share resources.
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Network Security Scan	Process by which an entity’s systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.
Network Segmentation	Means of reducing the scope of a PCI DSS assessment by reducing the size of the cardholder data environment. To achieve this, systems that do not store, process, or transmit cardholder data should be isolated from those systems that store, process, and transmit cardholder data via network controls. See Network Segmentation section in the *PCI DSS Requirements and Security Assessment Procedures* for guidance on using network segmentation.

NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration. Their mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life.
NMAP	Security-scanning software that maps networks and identifies open ports in network resources.
Non-Consumer Users	Individuals, excluding cardholders, who access system components, including but not limited to employees, administrators, and third parties.
NTP	Acronym for "network time protocol." Protocol for synchronizing the clocks of computer systems over packets switched, variable-latency data networks.
Off-the-Shelf	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Operating System/OS	Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.
OWASP	Acronym for "Open Web Application Security Project." A non-profit organization established in 2004 focused on improving the security of application software. OWASP released the OWASP Top Ten, which lists the most critical vulnerabilities for web applications. (See http://www.owasp.org).
PA-QSA	Acronym for "Payment Application Qualified Security Assessor," company approved by the PCI SSC to conduct assessments on payment applications against the PA-DSS.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Password/Passphrase	A string of characters that serve as an authenticator of the user.
Pad	In cryptography, the one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain-text and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable
PAT	Acronym for "port address translation" and also referred to as "network address port translation." Type of *NAT* that also translates the port numbers.
Patch	Update to existing software to add functionality or to correct a defect.
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.
PCI	Payment Card Industry.
PDA	Acronym for "personal data assistant" or "personal digital assistant." Handheld mobile devices with capabilities such as mobile phones, e-mail, or web browser.
Penetration Test	Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

PIN	Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
Private Network	Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers.
Procedure	Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.
Protocol	Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.
Public Network	Network established and operated by a telecommunications provider, for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks in scope of the PCI DSS include, but are not limited to, the Internet, wireless, and mobile technologies.
PVV	Acronym for "PIN verification value." Discretionary value encoded in magnetic stripe of payment card.
QSA	Acronym for "Qualified Security Assessor," company approved by the PCI SSC to conduct PCI DSS on-site assessments.
RADIUS	Abbreviation for "remote authentication and dial-in user service." Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system.
RBAC	Acronym for "role-based access control." Control used to restrict access by specific authorized users based on their job responsibilities.
Remote Access	Access to computer networks from a remote location, typically originating from outside the network. An example of technology for remote access is *VPN*.
Removable Electronic Media	Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.
Report on Compliance	Also referred to as "ROC." Report containing details documenting an entity's compliance status with the PCI DSS.
Report on Validation	Also referred to as "ROV." Report containing details documenting a payment application's compliance with the PCI PA-DSS.
Re-keying	Process of changing cryptographic keys to limit amount of data to be encrypted with the same key.

Risk Analysis/Assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
Rootkit	Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.
Sanitization	Process for deleting sensitive data from a file, device, or system; or for modifying data so that it is useless if accessed in an attack.
SANS	Acronym for "SysAdmin, Audit, Networking and Security," an institute that provides computer security training and professional certification. (See www.sans.org.)
SDLC	Acronym for "system development life cycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation.
Secure Wipe	Also called "secure delete," a program utility used to delete specific files permanently from a computer system.
Security Officer	Primary responsible person for security related affairs of an organization.
Security Policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information
SAQ	Acronym for "Self-Assessment Questionnaire." Tool used by any entity to validate its own compliance with the PCI DSS.
Sensitive Area	Any data center, server room or any area that houses systems that stores, processes, or transmits cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
Sensitive Authentication Data	Security-related information (card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.
Separation of Duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.
Server	Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.
SHA-1/SHA-2	Acronym for "Secure Hash Algorithm." A family or set of related cryptographic hash functions including SHA-1 and SHA-2. See *Strong Cryptography.*
Smart Card	Also referred to as "chip card" or "IC card (integrated circuit card)." A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the "chip," contain payment card data including, but not limited to, data equivalent to the magnetic-stripe data.
SNMP	Acronym for "Simple Network Management Protocol." Supports monitoring of network attached devices for any conditions that warrant administrative attention.
Split Knowledge	Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
Spyware	Type of malicious software that when installed, intercepts or takes partial control of the user's computer without the user's consent.
SQL	Acronym for "Structured Query Language." Computer language used to create, modify, and retrieve data from relational database management systems.
SQL Injection	Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
SSH	Abbreviation for "secure shell." Protocol suite providing encryption for network services like remote login or remote file transfer.
SSL	Acronym for "secure sockets layer." Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel.
Stateful Inspection	Also called "dynamic packet filtering," it is a firewall capability that provides enhanced security by keeping track of communications packets. Only incoming packets with a proper response ("established connections") are allowed through the firewall.
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). SHA-1 is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (http://csrc.nist.gov/publications/) for more information.

SysAdmin	Abbreviation for "system administrator." Individual with elevated privileges who is responsible for managing a computer system or network.
System Components	Any network component, server, or application included in or connected to the cardholder data environment.
TACACS	Acronym for "terminal access controller access control system." Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network.
TCP	Acronym for "Transmission Control Protocol." Basic communication language or protocol of the Internet.
TDES	Acronym for "Triple Data Encryption Standard" and also known as "3DES" or "Triple DES." Block cipher formed from the DES cipher by using it three times. See *Strong Cryptography.*
TELNET	Abbreviation for "telephone network protocol." Typically used to provide user-oriented command line login sessions to devices on a network. User credentials are transmitted in clear text.
Threat	Condition or activity that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization
TLS	Acronym for "transport layer security." Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Token	Hardware or software that performs dynamic or two-factor authentication.
Transaction Data	Data related to electronic payment card transaction.
Trojan	Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.
Truncation	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data.
Trusted Network	Network of an organization that is within the organization's ability to control or manage.
Two-Factor Authentication	Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).
Untrusted Network	Network that is external to the networks belonging to an organization and which is out of the organization's ability to control or manage.
VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network.
VPN	Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption.

Vulnerability	Weakness in a system that allows a malicious individual to exploit that system and violate its integrity.
WAN	Acronym for "wide area network." Computer network covering a large area, often a regional or company wide computer system.
Web Server	Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).
WEP	Acronym for "wired equivalent privacy." Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes. See *WPA.*
Wireless Access Point	Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.
Wireless Networks	Network that connects computers without a physical connection to wires.
WLAN	Acronym for "wireless local area network." Local area network that links two or more computers or devices without wires.
WPA/WPA2	Acronym for "WiFi Protected Access." Security protocol created to secure wireless networks. WPA is the successor to WEP and is deemed to provide better security than WEP. WPA2 was also released as the next generation of WPA.