sysnet global solutions

The Small Business A-Z of Cyber Security

Common terms definitions for your small business

Print and keep on your premises - make sense of the jargon around cybersecurity and the PCI DSS.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the symbol above.

Cyber security and small business

Welcome to the Small Business A-Z of Cybersecurity – you've taken your first step to understanding this complicated area of business management.

Cyber security, and by association compliance with the Payment Card Industry Data Security Standard (PCI DSS) are not items traditionally very high on the agenda of any small business owner. However, in recent times, that has seen an unprecedented amount of cyber security breaches in small and large business, it's time all businesses sat up and took notice – regardless of your size, location and industry.

Cyber security is a wide-ranging term that can relate to a plethora of complicated issues that are far above the head of the average person. However, what many people fail to understand is that a small business can take huge strides towards making itself secure by taking simple steps to secure their information such as strong password use and avoiding negligent security habits.

Using this guide

This guide, is a simple A-Z of the terms you hear when cyber security or PCI DSS is discussed. Some terms are simple, some more complicated so don't worry if you see things you don't understand, we have catered for all levels of expertise in this guide. It is not designed to be read from start to finish. Simply keep it on your desktop or print it off and keep it in your office. When you hear a term you don't understand, simply pick it up and look it up – you're one step closer to securing your business.

To quickly find a term: open this guide and press "Ctrl F" on your keyboard. This will open the find function on your PDF. Type the term you are looking for into the search box and the term will appear if it is included. Alternatively, you can use the magnifying glass icon in the top left of the screen to search for a term.

We hope you enjoy using this guide and find it useful.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Acronym/Term	*Explanation*
Access control	Mechanisms that limit availability of information or information-processing resources only to authorised persons or applications.
Account data	Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data.*
Account number	See *Primary Account Number (PAN).*
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Advanced Endpoint Protection (AEP)	Comprehensive security software that defends a customer's endpoints (See Endpoints) from potential infection leveraging containerisation technology.
Advanced Persistent Threat (APT)	APT is a targeted attack by an attacker with resources and time to infiltrate a network and remain there undetected for long periods of time. The intention of APT is to steal data or conduct reconnaissance for latter attacks intended to disrupt or damage a network.
Adware	Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.
AI / Machine Learning	Smart learning features allow the software to effectively learn from threats and viruses found by using artificial intelligence to block similar malicious files without the need to constantly update meaning the software can stay ahead of new threats
Anonymous proxy	A server which allows a user to hide their web browsing activity by hiding the IP address of the user's pc to the website. This can be a liability for organisations where their computers have been used to incite illegal behaviour or view inappropriate content.
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. It's important to have a strong AV program operating on all your business' machines.
AOC	Acronym for "attestation of compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.
AOV	Acronym for "attestation of validation." The AOV is a form used by a Payment Application Qualified Security Assessor (PA-QSA) to attest to the results of an assessment of a company's payment acceptance channels.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Application	An application is a software program that runs on your computer. Web browsers, e-mail programs, word processors and games are all applications. The word "application" is used because each program has a specific application for the user.
Application control	Selectively allow or block certain applications from accessing the Internet.
Application intelligent networking	Application intelligent networking refers to defensive security software that uses intelligence to ascertain whether a file or piece of code is malicious. When traditional anti-virus is deciding if a file is malicious it scans the file and checks it against a list of known bad files. Intelligent networking uses dynamic practices to examine the file's signature and checks it for anything unusual to decide if the file is safe to open.
Approved Scanning Vendor (ASV)	An ASV is an organisation with a set of security services and tools ("ASV scan solution") to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. Sysnet is an ASV company.
ASV Vulnerability Scanning	Helps assess the security position of any internet facing systems, checking external networks for gaps and vulnerabilities as per the requirements of the PCI DSS.
Attestation of compliance	A declaration of a merchant's compliance with the PCI DSS.
Audit log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of a sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Audit trail	See *Audit log.*
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs using one or more authentication factors such as: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as biometric (E.g. voice recognition, finger print recognition)
Authentication credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process. *(See Authentication)*

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Authorisation	In the context of access control, authorisation is the granting of access or other rights to a user, program, or process. Authorisation defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorisation occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Backdoor	A way of secretly bypassing normal authentication mechanisms and gaining unauthorised access to systems and processes and can be a method of inserting malware into a system.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
BAU	An acronym for "business as usual." BAU is an organisation's normal daily business operations.
Behavioural analysis	Behavioural analysis detects and blocks unusual activity on devices. The software will log normal network activity and monitor systems for any unusual activity (e.g. removal of large amounts of data). This is to block potential hacking activities or other malware from causing damage to systems.
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
Boot sector malware	Malware that is resident in the boot sector of a hard disk can affect the normal start-up operation of a system and can execute malicious code during start-up which prevents anti-virus mechanisms from starting.
Botnet	A botnet is a group of internet connected devices that are being remotely controlled by a hacker. The intention of a botnet is to send spam, steal data or take part in a distributed denial of service (DDoS) attack.
Browser hijack	Browser hijacking is a method of modifying the browsers setting without the user's consent, with the intention of forcing hits to a website to increase its revenue, steal data or to install key loggers to gather information.
Brute force attack	An attacker tries as many passwords or passphrases as possible with the aim of eventually guessing correctly and gaining unauthorised access to a system.
Buffer overflow	Vulnerability that is created from insecure coding methods, where a program overruns the buffer's boundary and writes data to adjacent memory space. Buffer overflows are used by attackers to gain unauthorised access to systems or data.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Card skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
Card verification code or value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. Data element on a card's magnetic stripe that uses secure cryptographic processes 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) 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 un-embossed 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 list provides the terms for each card brand: • **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)
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorised to use the payment card.
Cardholder data	At a minimum, cardholder data consists of the full PAN *(See PAN).* Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Cardholder data scan	Scans a company's network, files and folders to locate suspected payment card (PAN) data. The PCI DSS forbids the storing of unencrypted credit card details on a company's systems.
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Cellular technologies	Mobile communications through wireless telephone networks, including but not limited to Global System for Mobile communications (GSM), code division multiple access (CDMA), and General Packet Radio Service (GPRS).
CERT	Acronym for Carnegie Mellon University's "Computer Emergency Response Team." The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.
Change control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.
Change detection mechanism	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 as it could mean a data breach.
CIS	Acronym for "Centre for Internet Security." Non-profit enterprise with mission to help organisations 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.*
Command and control	Command and control software is used by an attacker to control a botnet.
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 defence 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.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Compromise	Also referred to as "data compromise," or "data breach." A compromise is considered to have occurred when the security of the system or data has been broken. A breach is any occurrence that has led to the compromise and usually occurs when security controls are bypassed or thwarted. Unauthorised intrusion into a computer system (a breach) may lead to disclosure/theft, modification, or destruction of cardholder data (i.e. a compromise). Compromises may occur as a result technology or system vulnerabilities, physical loss/theft or inadequacies/failures of business processes.
Console	Screen and keyboard which permits access and control of a server, mainframe computer or other system type in a networked environment.
Consumer	Individual purchasing goods, services, or both.
Containerisation	Unrecognised and potentially dangerous files are automatically placed within a secure container. They run in a restricted environment protecting your network from infection from malicious files. Once files have been analysed, safe files are released into the operating environment and malicious files are secured in a vault. Differs from anti-virus as does not rely on signature-based checks.
Core Model	Detection vs Prevention. This refers to the basic operation of defensive software in operation – the core model of operation. E.g. does the software prevent malware from entering or does it detect and remove it?
Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated/logged in. An attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.
Cross-Site Scripting (XSS)	Vulnerability that is created from insecure coding techniques, resulting in improper input validation (meaning the information supplied by the user cannot be verified as correct e.g. passwords, databases, code etc.). Often used in conjunction with *CSRF* and/or *SQL injection*.
Cryptographic key management	The set of processes and mechanisms which support *cryptographic key* establishment and maintenance, including replacing older keys with new keys as necessary.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Cryptographic key	Refers to *encryption* - a value that determines the output of an encryption algorithm when transforming plain text to ciphertext (i.e. the key to decipher the encryption). The length of the key determines how difficult it will be to decrypt the ciphertext in a given message. See *Strong Cryptography.*
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.
Crypto period	The time span during which a specific *cryptographic key* can be used for its defined purpose based on, for example, a defined period and/or the amount of cipher-text that has been produced, and according to industry best practices and guidelines (for example, *NIST Special Publication 800-57*).
CVSS	Acronym for "Common Vulnerability Scoring System." A vendor agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response. The higher the score, the more serious the vulnerability. Refer to *ASV Program Guide* for more information.
Data breach protection	If a breach occurs or is suspected, a forensic investigation may be required which can be disruptive to business and may result in the organisation paying for the analysis, additionally if there is non-compliance there may also be hefty fines. Data breach expenses can include the cost of a forensic audit, replacement of compromised cards, related expenses, and compliance fines and assessments levied by the card schemes; this can be enough to bankrupt a small business. Data Breach Protection can be taken out to help mitigate these costs.
Data loss prevention software	A method of monitoring and detecting potential software breaches and preventing them by blocking the sensitive data whilst 'in use on the endpoint, 'in motion' network traffic and 'at rest' whilst in storage.
Data migration	The movement of data from one system to another.
Database	Structured format for organising 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.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Data-flow diagram	A diagram showing how data flows through an application, system, or network. A specific diagram for cardholder data is needed to complete PCI DSS validation.
DDoS	A Distributed Denial of Service (DDoS) (also Dos) attack is an attack on a website whereby hackers overload the site with fake web traffic with the intention of it crashing due to an overload. This can be mitigated against with the application of a WAF (See Web Application Firewall)
Default accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default password	Password on system administration, user, 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. It is recommended to change your default password to one that is longer and more complicated when first logging in – never leave your default password as is.
Degaussing	Also called "disk degaussing." Process or technique that demagnetises the disk such that all data stored on the disk is permanently destroyed.
Dependency	In the context of *PA-DSS*, a dependency is a specific software or hardware component (such as a hardware terminal, database, operating system, API, code library, etc.) that is necessary for the payment application to meet *PA-DSS* requirements.
Desktop firewall	High-level security against inbound and outbound threats, blocking confidential data transmission by malicious software.
Device security scan	Comprehensively scans devices for vulnerabilities, assessing threats and vulnerabilities for OS versions as well as other applications on the device. The scan discovers and highlights data that may pose a compliance risk or contain security flaws.
Disk encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, *File Level Encryption* or *Column-Level Database Encryption* is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarised zone." Physical or logical sub-network that provides an additional layer of security to an organisation's internal private network. The DMZ adds an additional layer of network security so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

DNS	Acronym for "domain name system" or "domain name server." A system that stores information associated with domain names (E.g. www.example.com) in a distributed database to provide name-resolution services to users on networks such as the Internet.
DNS hijack	An attacker changes a system's settings to ignore its own DNS or redirect traffic to one controlled by an attacker. Often used in spam email to redirect user to a fake login page for banks or online stores in order to steal their login credentials.
Drive by download	A method of infecting a system with malware when a user visits a website. Hackers often attack legitimate websites and inject them with malicious code which is subsequently passed into other browsers visiting that website.
DSS	Acronym for "Data Security Standard." See *PA-DSS* and *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) that require shorter encryption keys with equivalent protection. See *Strong Cryptography.*
Egress filtering	Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the 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 unauthorised disclosure. See *Strong Cryptography.*
Encryption algorithm	Also called "cryptographic algorithm." A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again. See *Strong Cryptography.*
Endpoint containment firewall	Filters traffic to/from Windows workstations and servers, allowing known safe applications to communicate while blocking or alerting on any suspicious activity.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Endpoints	Refers to the devices used in an organisation i.e. mobile phones, POS terminals, laptops, tablets etc. These devices need to be protected against secure vulnerabilities as many connect to the main network of the business.
Entity	Term used to represent the corporation, organisation or business which is undergoing a *PCI DSS* review.
Exploit	A piece of software, data or sequence of commands that take advantage of a vulnerability in a system to cause unanticipated behaviour in that system leaving an attacker able to compromise it.
External (network) vulnerability scanning	Helps assess the security position of any internet facing systems, checking external network for gaps and vulnerabilities. It is requirement 11.2 of the PCI DSS.
Fake malware or scareware	Fake malware is used to scare users into downloading and installing unnecessary software. It will report non-existent vulnerabilities or threats, tricking the user into paying for an unnecessary product.
File integrity monitoring	Technique or technology under which certain files or logs are monitored to detect if they have been modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel as it could mean a security breach. i.e. someone has changed parts of your computer system without the proper authority.
File monitoring	Instant analysis of unknown files that checks file reputation against master whitelist and blacklists.
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 recognised by the U.S. Federal Government; also for use by nongovernment agencies and contractors.
Firewall	Hardware and/or software technology that protects network resources from unauthorised access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria. A firewall is a very useful form of defence against hackers and malware as it prevents access to your system by anyone/anything deemed malicious.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Forensics	Also referred to as "computer forensics." 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. See *S-FTP*.
GPRS	Acronym for "General Packet Radio Service." Mobile data service available to users of GSM mobile phones. Recognised 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.
Hacktivists and hacktivism	Hacktivism is a movement of people who seek to promote a political agenda by defacing websites, stealing information, redirecting traffic and launching denial-of-service attacks in support of their cause.
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed length message digest via *Strong Cryptography.* Hashing is a one-way (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). A hash function should have the following properties: 1. It is computationally infeasible to determine the original input given only the hash code 2. It is computationally infeasible to find two inputs that give the same hash code. In the context of PCI DSS, hashing must be applied to the entire *PAN* for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data include an input variable (for example, a "salt") to the hashing function to reduce or defeat the effectiveness of pre-computed rainbow table attacks (see *Input Variable*).

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Honeypot	A cyber security measure to entice hackers into a computer system with the intention of capturing malware, detect attacks or provide fake network services with the intention of monitoring the motives and tactics of hackers by 'baiting' a system to make it look genuine and potentially valuable.
Host	Main computer hardware on which computer software is resident.
Host Intrusion Prevention (HIPs)	Monitors important operating system activities to ensure protection against malware intrusion.
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.
HSM	Acronym for "hardware security module" or "host security module." A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data.
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.
Hypervisor	Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM).
ID	Identifier for a user or application.
IDS	Acronym for "intrusion-detection system." Software or hardware used to identify and alert on network or system anomalies or 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 detected security events. See *IPS.*

sysnet global solutions

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

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.
IMAP	Acronym for "Internet Message Access Protocol." An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
Index token	A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information system	Discrete set of structured data resources organised for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information security	Protection of information to ensure confidentiality, integrity, and availability.
Ingress filtering	Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network.
Injection flaws	Vulnerability that is created from insecure coding techniques resulting in improper input validation (validating that code or information input by a user is accurate or correct e.g. passwords), which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection.
Input variable	Random data string that is concatenated with source data before a one-way hash function is applied. Input variables can help reduce the effectiveness of rainbow table attacks. See also *Hashing* and *Rainbow Tables.*
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 or authentication credentials (for example, password/passphrase) in clear-text over the Internet, or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed and delivered from the source host to the destination host. IP is the primary network layer protocol in the Internet protocol suite. See *TCP*.
IP address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a computer (host) on the Internet.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

IP address spoofing	Attack technique used to gain unauthorised access to networks or 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 at the network layer by encrypting and/or authenticating all IP packets in a communication session.
ISO	Better known as "International Organisation for Standardisation." Nongovernmental organisation consisting of a network of the national standards institutes.
Issuer	Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as "issuing bank" or "issuing financial institution."
Issuing services	Examples of issuing services may include but are not limited to authorisation and card personalisation.
Keylogger	A method of capturing keyboard keystrokes covertly in order to steal information such as passwords.
LAN	Acronym for "local area network." A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.
LDAP	Acronym for "Lightweight Directory Access Protocol." Authentication and authorisation data repository utilised for querying and modifying user permissions and granting access to protected resources.
Least privilege	Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.
Log	See *Audit Log.*
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	In cryptography, an acronym for "message authentication code." 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	See *Track Data.*
Mainframe	Computers that are designed to handle very large volumes of data input and output and emphasise 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 or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Similar examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Malware detection (file less / file based)	Malware is a piece of code that runs on a system for a malicious purpose. File less malware is malicious code that does not have a host file but runs in the system's memory and is much more difficult to detect than its traditional file-based cousin.
Managed Security Services (MSS)	The act of outsourcing your security to a third-party provider. Often provides many benefits to managing security in-house as due to the complexity of security issues and the shortage of skilled security staff.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See *Truncation* for protection of PAN when stored in files, databases, etc.
Memory-scraping attacks	Malware activity that examines and extracts data that resides in memory as it is being processed or which has not been properly flushed or overwritten.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

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.
MO/TO	Acronym for "Mail-Order/Telephone-Order."
Mobile device security management	Managing the security of a company's mobile devices to ensure no security vulnerabilities exist or that they are mitigated against. Involves regular scanning and the application of defensive software amongst other measures.
Mobile device security scan	Comprehensively scans mobile devices for vulnerabilities, assessing threats and vulnerabilities for OS versions as well as other applications on the device. The scab discovers and highlights data that may pose a compliance risk or contain security flaws.
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.
NAC	Acronym for "network access control" or "network admission control." A method of implementing security at the network layer by restricting the availability of network resources to *endpoint* devices (mobiles, computers etc.) according to a defined security policy.
NAT	Acronym for "network address translation." Also 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, allowing an organisation to have internal addresses that are visible internally, and external addresses that are only visible externally.
Network	Two or more computers connected via physical or wireless means.
Network administrator	Personnel responsible for managing the network within an entity. Responsibilities typically include but are not limited to; network security, installations, upgrades, maintenance and activity monitoring.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Network appliance	Typically an inexpensive personal computer, sometimes called a thin client, that enables Internet access and some business-related activities but lacks many features of a fully equipped PC, such as a hard drive or CD-ROM.
Network components	Include, but are not limited to *firewalls, switches, routers, wireless access points, network appliances*, and other security appliances.
Network segmentation	Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the *PCI DSS Requirements and Security Assessment Procedures* for guidance on using network segmentation.
Network (host) discovery	Discovers all devices in use on a network, alerting the system administrator to unauthorised devices that have access to the system.
Network diagram	A diagram showing system components and connections within a networked environment.
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 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 sniffing	Also referred to as "packet sniffing" or "sniffing." A technique that passively monitors or collects network communications, decodes protocols, and examines contents for information of interest.
NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.
NMAP	Security-scanning software that maps networks and identifies open ports in network resources.

sysnet global solutions

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Non-console administrative access	Refers to logical administrative access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console administrative access includes access from within local/internal networks as well as access from external, or remote, networks.
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 synchronising the clocks of computer systems, network devices and other system components.
NVD	Acronym for "National Vulnerability Database." The U.S. government repository of standards-based vulnerability management data. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
OCTAVE®	Acronym for "Operationally Critical Threat, Asset, and Vulnerability Evaluation." A suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.
Off-the-shelf	Description of products that are stock items not specifically customised 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.
Organisational independence	An organisational structure that ensures there is no conflict of interest between the person or department performing the activity and the person or department assessing the activity. For example, individuals performing assessments are organisationally separate from the management of the environment being assessed.
OWASP	Acronym for "Open Web Application Security Project." A non-profit organisation focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (See http://www.owasp.org).
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.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

PA-DSS	Acronym for "Payment Application Data Security Standard." The global security standard created by the PCI SSC. It is a standard provides definitive guidelines for software vendors that develop payment applications. The standard aims to prevent the storing of secure card data by third parties and says payment acceptance software should be compliant with the PCI 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.
PA-QSA	Acronym for "Payment Application Qualified Security Assessor." PA-QSAs are qualified by PCI SSC to assess payment applications against the PA-DSS. Refer to the *PA-DSS Program Guide* and *PA-QSA Qualification Requirements* for details about requirements for PA-QSA Companies and Employees.
Parameterised queries	A means of structuring SQL queries to limit escaping and thus prevent injection attacks.
Parasitic virus	A virus which piggybacks itself to a program and when the program is run, the virus code is also run with the same permissions as the program, giving it rights which allow it to replicate, install itself into memory and make changes to the computer.
Password / Passphrase	A string of characters that serve as an authenticator of the user. Passwords/Passphrases should be long rather than short and should use a mixture of upper and lower-case letters, numbers and symbols. Passwords should be changed frequently, at least every 90 days. Passphrases are more difficult to crack than passwords. For example, 'Spiderm@n, m0vie' takes a lot longer to crack than 'Spiderman12!'.
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 application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorisation or settlement, where the payment application is sold, distributed, or licensed to third parties. Refer to *PADSS Program Guide* for details.
Payment Card Industry Data Security Standard (PCI DSS)	The Payment Card Industry Data Security Standard (PCI DSS) is a set of minimum security requirements that must be met to handle payment card information securely. The card brands (MasterCard, Visa, American Express, Discover and JCB) require that any business accepting cards for payment must be compliant with the PCI DSS.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Payment Card Industry Security Standards Council (PCI SSC)	The PCI SSC is the council which oversees the PCI DSS. The council maintains, evolves and promotes Payment Card Industry standards for the safety of cardholder data across the globe.
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	Acronym for "Payment Card Industry."
PCI DSS	Acronym for "Payment Card Industry Data Security Standard." The Payment Card Industry Data Security Standard (PCI DSS) is a set of minimum security requirements that must be met to handle payment card information securely. The card brands (MasterCard, Visa, American Express, Discover and JCB) require that any business accepting cards for payment must be compliant with the PCI DSS. Core to the PCI DSS is protecting customers' payment card data.
PDA	Acronym for "personal data assistant" or "personal digital assistant." Handheld mobile devices with capabilities such as mobile phones, e-mail, or web browser.
PED	Acronym for "PIN Entry Device."
Penetration test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. A Penetration Test is an attempt by an individual or "Ethical Hacker" to exploit a company's system using, as close as possible, the methods employed by real hackers. The result of a Penetration Test should inform a company of areas of its network defences it needs to improve to remain secure.
Personal firewall software	A software firewall product installed on a single computer.
Personally Identifiable Information (PII)	Information that can be utilised to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, etc.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.
Phishing	Phishing is the practice of a hacker attempting to fool an unsuspecting user into accessing a malicious link or downloading an infected file through the practice of *Social Engineering*. E.g.: A Hacker will send an email to an employee pertaining to be from a legitimate business with offers via "The link below" or in "The attachment." The unsuspecting employee clicks the link or opens the attachment which then downloads malware or ransomware. As the user allows the code to download or the link to execute, this can enable the malware to bypass traditional anti-virus software or inadequate firewalls, heightening the impact.
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.
POI	Acronym for "Point of Interaction," the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.
Policy	Organisation-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
Port	Logical (virtual) connection points associated with a communication protocol to facilitate communications across networks.
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
POS terminals	Point-of-Sale terminals – the device used by a merchant to accept payment from their customer.
Private network	Network established by an organisation 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*.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Privileged user	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary depending on the organisation, job function or role, and the technology in use.
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.
Proxy server	A server that acts as an intermediary between an internal network and the Internet. Proxy servers can be used for various purposes, such as sharing Internet connections on a local area network, hiding IP addresses, implementing Internet access control, accessing blocked websites etc.
PTS	Acronym for "PIN Transaction Security," PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org
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. E.g. the Internet.
PVV	Acronym for "PIN verification value." Discretionary value encoded in the magnetic stripe of a payment card.
QIR	Acronym for "Qualified Integrator or Reseller." Refer to the *QIR Program Guide* on the PCI SSC website for more information.
QSA	Acronym for "Qualified Security Assessor." QSAs are qualified by *PCI SSC* to perform *PCI DSS* on-site assessments. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees.
Qualified Security Assessor (QSA)	The term QSA can be implied to identify an individual qualified to perform payment card industry compliance auditing and consulting or the firm itself (Sysnet is a QSA company and employees QSA individuals). QSA companies are sometimes differentiated from QSA individuals by the initialism 'QSAC'

	The primary goal of an individual with the PCI QSA certification is to perform an assessment of a firm that handles credit card data against the high-level control objectives of the PCI Data Security Standard (PCI DSS).
RADIUS	Abbreviation for "Remote Authentication Dial-In User Service" authentication and accounting system. Checks if information such as a username and password that is passed to the RADIUS server is correct, and then authorises access to the system. This authentication method may be used with a token, smart card, etc., to provide *two-factor authentication*.
Rainbow table attack	A method of data attack using a pre-computed table of *hash strings* (fixed-length message digest) to identify the original data source, usually for cracking password or cardholder data hashes.
Ransomware	Ransomware is a form of malware that infects a victim's system by encrypting or blocking access to all folders and files on the user's network. The victim must then pay money (i.e. a ransom) to the owner of the Ransomware for them to restore access to the blocked files. This can be particularly troublesome for many businesses who rely on their computers and the files stored on them to operate. It is a favourite with organised hacking groups as it gives them easy access to revenue to fund their extensive efforts.
Re-keying	Process of changing *cryptographic keys*. Periodic re-keying limits the amount of data encrypted by a single key.
Remote access	Access to computer networks from a remote location. Remote access connections can originate either from inside the company's own network or from a remote location outside the company's network. An example of technology for remote access is a *VPN (Virtual Private Network)*.
Remote lab environment	A lab that is not maintained by a PA-QSA.
Removable electronic media	Media that store digitised 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.
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
RFC 1918	The standard identified by the Internet Engineering Task Force (IETF) that defines the usage and appropriate address ranges for private (non-internet routable) networks.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Risk analysis / Risk assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimise total exposure.
Risk ranking	A defined criterion of measurement based upon the risk assessment and risk analysis performed on a given entity.
ROC	Acronym for "Report on Compliance." Report documenting detailed results from an entity's PCI DSS assessment.
Rootkit	Type of malicious software that when installed without authorisation, can 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.
ROV	Acronym for "Report on Validation." Report documenting detailed results from a *PA-DSS* assessment for purposes of the *PA-DSS* program.
Runtime protection	A monitoring system within your computer designed to analyse the behaviour of the programs already running within your computer for signs of anomalous behaviour and blocks any activity which could be malicious. Also checks the Windows registry for signs that malware may be trying to install itself.
Sampling	The process of selecting a cross-section of a group that is representative of the entire group. Sampling may be used by assessors to reduce overall testing efforts, when it is validated that an entity has standard, centralised PCI DSS security and operational processes and controls in place. Sampling is not a PCI DSS requirement.
SANS	Acronym for "SysAdmin, Audit, Networking and Security," an institute that provides computer security training and professional certification. (See http://www.sans.org/.)
SAQ	Self-Assessment Questionnaire. Refers to the questionnaire a merchant completes to ascertain whether they are compliant with the PCI DSS. A merchant assesses themselves against the elements of the standard to judge their compliance. Once assessed they are given a category into which they fit (e.g. SAQ A, SAQ B etc.)

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Schema	Formal description of how a database is constructed including the organisation of data elements.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.
SDLC	Acronym for "system development life cycle" or "software development lifecycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation.
Secure cryptographic device	A set of hardware, software and firmware that implements *cryptographic processes* (including cryptographic algorithms and key generation) and is contained within a defined cryptographic boundary. Examples of secure cryptographic devices include host/hardware security modules (HSMs) and point-of-interaction devices (POIs) that have been validated to PCI PTS.
Secure CDN	A content delivery network or content distribution network (CDN) is a network of servers and data centres that distribute content to the user based on their geographic location.
Secure coding	The process of creating and implementing applications that are resistant to tampering and/or compromise by a hacker or malicious software.
Secure POS malware protection	An extra layer of protection: runs user sessions inside non-modifiable containers that treat all other active computing processes as hostile. This keeps applications (such as payment apps) safe and isolated on their host devices and can run uninterrupted, even on infected devices.
Secure wipe	Also called "secure delete," a method of overwriting data residing on a hard disk drive or other digital media, rendering the data irretrievable.
Security event	An occurrence considered by an organisation to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity.
Security officer	Primary person responsible for an entity's security-related matters.
Security policy	Set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes sensitive information.
Security protocols	Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to SSL/TLS, IPSEC, SSH, HTTPS, etc.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Sensitive authentication data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorise payment card transactions.
Sensitive area	Any data centre, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
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.
S-FTP	Acronym for Secure-FTP. S-FTP has the ability to encrypt authentication information and data files in transit. See *FTP.*
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.*
SIEM	Security Incident and Event Management (SIEM) is a term used to describe the constant monitoring of a company's security defences and systems. Often a piece of monitoring software that alerts security experts to potentially harmful activity on a company's network. Often suited to companies with high levels of resources needing to protect value information.
SIEM integration	(See SIEM) In order for a SIEM to operate efficiently it needs to draw information from many different sources. Many security products such as anti-virus and firewalls offer the ability to integrate with SIEMs in order to provide them with information to make them a more effective operation.
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.
Social engineering	The methods attackers use to deceive victims into divulging confidential or personal information or performing an action such as following a link to a malicious website or opening a malicious file attachment.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

Spam	Unsolicited bulk email usually with the intention of tricking users to reveal sensitive information or make a purchase of something.
Spear phishing	A method of sending emails from what appear to be legitimate sources with the intention of tricking the targeted individuals to reveal sensitive information such as usernames and passwords.
Spoofing	Email spoofing is where the header of an email is a forgery and appears to have originated from somewhere other than the actual source. Commonly used in phishing and spear phishing attacks.
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 unauthorised 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 organisation'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. See *TLS.* Effectively means the web traffic you are viewing is secure and cannot be altered before reaching your screen.
Strong cryptography	Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). In essence it refers to a method whereby the true value of data is changed or disguised in order to prevent its unauthorised interception and use through the use of a code that disguises the data making it unusable by anybody who does not have access to the code or key.
Switches	Computer networking devices that are used to connect many devices together on a computer network. Switches create networks, allowing devices to talk to each other, while a Router connects networks.
Sysadmin	Abbreviation for "system administrator." Individual with elevated privileges who is responsible for managing a computer system or network.

sysnet global solutions

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

System components	Any network devices, servers, computing devices, or applications included in or connected to the cardholder data environment.
System-level object	Anything on a system component that is required for its operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.
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. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication.
TCP	Acronym for "Transmission Control Protocol." One of the core transport-layer protocols of the Internet Protocol (IP) suite, and the basic communication language or protocol of the Internet. See *IP*.
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 has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organisation.
TLS	Acronym for "Transport Layer Security." Designed with the goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Token	In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or two-factor authentication. See *RADIUS, TACACS,* and *VPN.*
Track data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorisation during payment transactions.
Transaction data	Data related to electronic payment card transaction.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

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. Truncation relates to protection of PAN when *stored* in files, databases, etc. See *Masking* for protection of PAN when *displayed* on screens, paper receipts, etc.
Trusted network	Network of an organisation that is within the organisation'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).
UI	User Interface – refers to the platform of a piece of software with which the customer or user interacts.
Unified Threat Management (UTM)	UTM brings multiple security functions into one place (cloud or appliance) such as firewall, content filtering, anti-virus, anti-spam, web application firewall and endpoint security management.
Untrusted Network	Network that is external to the networks belonging to an organisation and which is out of the organisation's ability to control or manage.
URL	Acronym for "Uniform Resource Locator." A formatted text string used by Web browsers, e-mail clients, and other software to identify a network resource on the Internet. Also known as a "link."
URL filtering / Web filtering	Creates rules to block certain types of potentially harmful websites and URLs. Can be applied via security software such as anti-virus packages or secure web gateways.
UX	User E**x**perience – how a user interacts with a piece of software. Does the user view the use of the software positively? This is their experience.
Versioning methodology	A process of assigning version schemes to uniquely identify a particular state of an application or software. These schemes follow a version-number format, version-number usage, and any wildcard element as defined by the software vendor. Version numbers are generally assigned in increasing order and correspond to a particular change in the software.

	It's important, as a business to use the latest version of any software you are using to ensure it is resistant to the latest security vulnerabilities.
Virtual Appliance (VA)	A VA is essentially a device that you use in your business to perform a specific function but is run virtually and is accessible via your network or the Internet. Examples would include a virtual router, switch or firewall.
Virtual hypervisor	See *Hypervisor*.
Virtual machine	A self-contained operating environment that behaves like a separate computer. E.g. a user can log into their virtual machine from any computer within or outside the company's network (depending on settings) and resume work as if they hadn't moved machines. Useful for remote working or companies employing hot desking.
Virtual Machine Monitor (VMM)	The VMM is included with the hypervisor and is software that implements virtual machine hardware abstraction. It manages the system's processor, memory, and other resources to allocate what each guest operating system requires. See Virtual Machine.
Virtual payment terminal	A virtual payment terminal is web-browser-based access to an acquirer, processor or third-party service provider website to authorise payment on a card transaction. The merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtualisation	Virtualisation refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualisation can be performed on many other computing resources, including applications, desktops, networks, and storage. See *Virtual Machine* for example.
Virus	A malicious piece of code that can cause a computer system to malfunction in a variety of ways. Can be defended against using anti-virus software. See Malware.

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network. See *LAN*.
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 tunnelled 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. A VPN may be used with a token, smart card, etc., to provide *two-factor authentication*.
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
Vulnerability management	Refers to the detection of the presence of known security vulnerabilities on business systems and devices and managing these. Also, can refer to the managing of the risk of these vulnerabilities.
WAN	Acronym for "wide area network." Computer network covering a large area, often a regional or company-wide computer system.
Web application	An application that is accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.
Web Application Firewall (WAF)	A layer of protection for a website. Blocks attacks on web server vulnerabilities, prevents disclosure of sensitive information and provides control over where and when applications are accessed.
Web server	Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages). i.e. the server that sends the information about the web page you are viewing to your computer screen when you request it via your browser.
Website blacklist monitoring & removal	The monitoring of websites being potentially blacklisted and then removing access to these websites that could be potentially harmful or that are intentionally attempting to spoof the user (e.g. Goolge).
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.*

Glossary of cyber security and PCI DSS terms

Use CTRL F to search for a term or click the 🔍 symbol above.

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.
Worm	A worm is a computer application, acting as a virus that replicates itself and then moves to another computer or system. It uses computer networks to replicate itself and thrives on systems without adequate defences in place. Again, antivirus software is a good place to start to defend against worms.
WPA/WPA2	Acronym for “Wi-Fi Protected Access.” Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA.
Zero-day defence	While anti-virus identifies known threats, zero-day defence features protects against unknown malware and potential threats. Involves analysis of every file in a secure portal to make sure that it isn't malicious before it can run on a user’s system (See Containerisation).