Payment Card Industry
Self-Assessment Questionnaire

How to Complete the Questionnaire

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard. For any questions where N/A is marked, a brief explanation should be attached.

Questionnaire Reporting

The following must be included with the self-assessment questionnaire and system perimeter scan results:

Organization Information

CORPORATE NAME:		DBA(S):	
CONTACT NAME:		TITLE:	
PHONE:		E-MAIL:	
APPROXIMATE NUMBER OF TRANSACTIONS/ACCOUNTS HANDLED PER YEAR:			

Please include a brief description of your business.

Please explain your business' role in the payment flow. How and in what capacity does your business store, process and/or transmit cardholder data?

List all Third Party Service Providers

Processor:		Gateway:	
Web Hosting		Shopping Cart:	
Co-Location:		Other:	

List Point of Sale (POS) software/hardware in use:

Rating the Assessment

After completing each section of the assessment, users should fill in the rating boxes as follows:

IN EACH SECTION IF…	THEN, THE SECTION RATING IS …
ALL questions are answered with “yes” or “N/A”	**Green** - The merchant or service provider is compliant with the self-assessment portion of the PCI Data Security Standard. *Note: If “N/A” is marked, attach a brief explanation.*
ANY questions are answered with “no”	**Red** – The merchant or service provider is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

Section 1:	Green	Red	**Section 4:**	Green	Red
Section 2:	Green	Red	**Section 5:**	Green	Red
Section 3:	Green	Red	**Section 6:**	Green	Red
			Overall Rating:	**Green**	**Red**

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

DESCRIPTION		RESPONSE		
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	□ Yes	□ No	
1.2	If wireless technology is used, is the access to the network limited to authorized devices?	□ Yes	□ No	□ N/A
1.3	Do changes to the firewall need authorization and are the changes logged?	□ Yes	□ No	
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	□ Yes	□ No	
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	□ Yes	□ No	
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	□ Yes	□ No	
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?	□ Yes	□ No	□ N/A
1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	□ Yes	□ No	□ N/A
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?	□ Yes	□ No	
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?	□ Yes	□ No	

Build and Maintain a Secure Network

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

	DESCRIPTION	RESPONSE		
2.1	Are vendor default security settings changed on production systems before taking the system into production?	□ Yes	□ No	
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	□ Yes	□ No	
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?	□ Yes	□ No	□ N/A
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?	□ Yes	□ No	□ N/A
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?	□ Yes	□ No	
2.6	Are secure, encrypted communications used for remote administration of production systems and applications?	□ Yes	□ No	□ N/A

Protect Cardholder Data

Requirement 3: Protect stored data

	DESCRIPTION	RESPONSE
3.1	Is sensitive cardholder data securely disposed of when no longer needed?	□ Yes □ No
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?	□ Yes □ No
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?	□ Yes □ No
3.4	Are all but the last four digits of the account number masked when displaying cardholder data?	□ Yes □ No
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation?	□ Yes □ No
3.6	Are account numbers sanitized before being logged in the audit log?	□ Yes □ No

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

	DESCRIPTION	RESPONSE
4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	□ Yes □ No
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	□ Yes □ No □ N/A
4.3	If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?	□ Yes □ No □ N/A
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?	□ Yes □ No □ N/A
4.5	Is encryption used in the transmission of account numbers via e-mail?	□ Yes □ No □ N/A

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

DESCRIPTION		RESPONSE		
5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	□ Yes	□ No	

Requirement 6: Develop and maintain secure systems and applications

DESCRIPTION		RESPONSE		
6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	□ Yes	□ No	
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?	□ Yes	□ No	□ N/A
6.3	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?	□ Yes	□ No	□ N/A
6.4	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	□ Yes	□ No	
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	□ Yes	□ No	□ N/A
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	□ Yes	□ No	□ N/A
6.7	Is sensitive cardholder data stored in cookies secured or encrypted?	□ Yes	□ No	□ N/A
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	□ Yes	□ No	□ N/A

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

	DESCRIPTION	RESPONSE
7.1	Is access to payment card account numbers restricted for users on a need-to-know basis?	□ Yes □ No

Requirement 8: Assign a unique ID to each person with computer access

	DESCRIPTION	RESPONSE
8.1	Are all users required to authenticate using, at a minimum, a unique username and password?	□ Yes □ No
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?	□ Yes □ No □ N/A
8.3	Are all passwords on network devices and systems encrypted?	□ Yes □ No
8.4	When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?	□ Yes □ No
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	□ Yes □ No
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?	□ Yes □ No
8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed?	□ Yes □ No □ N/A
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer users?	□ Yes □ No
8.9	Are non-consumer users required to change their passwords on a pre-defined regular basis?	□ Yes □ No
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	□ Yes □ No
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	□ Yes □ No

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

	DESCRIPTION	RESPONSE
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	☐ Yes ☐ No
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?	☐ Yes ☐ No ☐ N/A
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	☐ Yes ☐ No
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	☐ Yes ☐ No
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	☐ Yes ☐ No
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	☐ Yes ☐ No
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	☐ Yes ☐ No

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

	DESCRIPTION	RESPONSE	
10.1	Is all access to cardholder data, including root/administration access, logged?	□ Yes	□ No
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	□ Yes	□ No
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?	□ Yes	□ No
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	□ Yes	□ No
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?	□ Yes	□ No

Requirement 11: Regularly test security systems and processes

	DESCRIPTION	RESPONSE		
11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?	□ Yes	□ No	□ N/A
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	□ Yes	□ No	
11.3	Is a intrusion detection or intrusion prevention system used on the network?	□ Yes	□ No	
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?	□ Yes	□ No	

Maintain a policy that addresses information security

Requirement 12: Maintain a policy that addresses information security

	DESCRIPTION	RESPONSE	
12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	□ Yes	□ No
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	□ Yes	□ No
12.3	Are information security policies reviewed at least once a year and updated as needed?	□ Yes	□ No
12.4	Have the roles and responsibilities for information security been clearly defined within the company?	□ Yes	□ No
12.5	Is there an up-to-date information security awareness and training program in place for all system users?	□ Yes	□ No
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	□ Yes	□ No
12.7	Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?	□ Yes	□ No
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	□ Yes	□ No
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	□ Yes	□ No
12.10	Are security incidents reported to the person responsible for security investigation?	□ Yes	□ No
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise?	□ Yes	□ No

Glossary

TERM	DEFINITION
Access control	Measures that limit access to information or information processing resources to those authorized persons or applications.
Account harvesting	A method to determine existing user accounts based on trial and error. Giving too much information in an error message can disclose information that makes it easier for an attacker to penetrate or compromise the system.
Account number	The payment card number (credit or debit) that identifies the issuer and the particular cardholder account.
Acquirer	A bankcard association member that initiates and maintains relationships with merchants that accept Visa or MasterCard cards.
Asset	Information or information processing resources of an organization.
Audit Log	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.
Authentication	The process of verifying identity of a subject or process.
Authorization	The granting of access or other rights to a user, program, or process
Backup	A duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Card-validation code	The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.
Cardholder	The customer to whom a card has been issued or the individual authorized to use the card.
Cardholder data	All personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered about the cardholder ‘i.e., addresses, telephone numbers, and so on).
Compromise	An intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.
Console	A screen and keyboard which allows access and control of the server / mainframe in a networked environment.
Consumer	Individual purchasing goods and /or services.
Cookies	A string of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information.
Database	A structured format for organizing and maintaining information that can be easily retrieved. A simple example of a database is a table or a spreadsheet.
DBA	Doing Business As. Compliance validation levels are based on the transaction volume of a DBA or chain of stores (not of a corporate that owns several chains).

Glossary

TERM	DEFINITION
Default accounts	A system login account that has been predefined in a manufactured system to permit initial access when the system is first put into service.
Default password	The password on system administration or service accounts when a system is shipped from the manufacturer, usually associated with the default account. Default accounts and passwords are published and well known.
Dual Control	A method of preserving the integrity of a process by requiring that several individuals independently take some action before certain transactions are completed.
DMZ (de-militarized zone)	A network added between a private network and a public network in order to provide an additional layer of security.
Egress	Traffic leaving the network.
Encryption	The process of converting information into a form unintelligible to anyone except 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.
Firewall	Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.
Host	The main hardware on which software is resident.
Information Security	Protection of information for confidentiality, integrity and availability.
Ingress	Traffic entering the network.
Intrusion detection Systems	An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
IP address	An IP address is a numeric code that uniquely identifies a particular computer on the Internet.
IP Spoofing	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
ISO 8583	An established standard for communication between financial systems.
Key	In cryptography, a key is a value applied using an algorithm to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during a card present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV, and Visa reserved values must be purged; however, account number, expiration date, and name may be extracted and retained.
Monitoring	A view of activity on a network.

Glossary

TERM	DEFINITION
Network	A network is two or more computers connected to each other so they can share resources.
Network Address Translation (NAT)	The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
Non consumer users	Any user, excluding consumer customers, that accesses systems, including but not limited to, employees, administrators, and third parties.
Password	A string of characters that serve as an authenticator of the user.
Patch	A quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems will almost invariably be found. A patch is the immediate solution that is provided to users.
Penetration	The successful act of bypassing the security mechanisms of a system.
Penetration Test	The security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit. The testing involves an attempt to penetrate the system so the tester can report on the vulnerabilities and suggest steps to improve security.
Policy	Organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
Procedure	A procedure provides the descriptive narrative on the policy to which it applies. It is the "how to" of the policy. A procedure tells the organization how a policy is to be carried out.
Protocol	An agreed-upon method of communication used within networks. A specification that describes the rules and procedures products should follow to perform activities on a network.
Risk Analysis	Also known as risk assessment, a process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., 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.
Router	A router is a piece of hardware or software that connects two or more networks. A router functions as a sorter and interpreter as it looks at addresses and passes bits of information to their proper destinations. Software routers are sometimes referred to as gateways.
Sanitization	To delete sensitive data from a file, a device, or a system; or modify data so that data is useless for attacks.
Security Officer	The person who takes primary responsibility for the security related affairs of the organization.
Security policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Glossary

TERM	DEFINITION
Sensitive cardholder data	Data whose unauthorized disclosure may be used in fraudulent transaction. It includes, the account number, magnetic stripe data, CVC2/CVV2 and expiration date.
Separation of duties	The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.
Server	A computer that acts as a provider of some service to other computers, such as processing communications, file storage, or printing facility.
SQL injection	A form of attack on a database-driven Web site in which the attacker 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.
SSL	An 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.
System Perimeter Scan	An automated tool that remotely checks a merchant's or service provider's systems for vulnerabilities. This non-intrusive test involves probing external-facing systems based on the external-facing Internet protocol (IP) addresses and reporting on the services available to the external network (i.e. services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.
Tamper-resistance	A system is said to be tamper-resistant if it is difficult to modify or subvert, even for an assailant who has physical access to the system.
Threat	A condition 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.
Token	A device that performs dynamic authentication.
Transaction data	Data related to an electronic payment.
Truncation	The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.
Two-factor authentication	Authentication that requires users to produce two credentials - something they have (e.g., smartcards or hardware tokens), and something they know (e.g., a password). In order to access a system, users must produce both factors.
UserID	A character string that is used to uniquely identify each user of a system.
Virus	A program or a string of code that can replicate itself and cause the modification or destruction of software or data.
Vulnerability	A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.
Vulnerability Scan	An automated tool that checks a merchant or service provider's systems for vulnerabilities. Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.