BIGCOMMERCE

The PCI Compliance Guide For Ecommerce

The PCI Compliance Guide For Ecommerce

Whether your company has been selling online for 20 minutes or 20 years, you are undoubtedly familiar with the PCI DSS (Payment Card Industry Data Security Standard). It requires merchants to create security management policies and procedures for safeguarding customers' payment data.

Originally created by Visa, MasterCard, Discover, and American Express in 2004, the PCI DSS has evolved over the years to ensure online sellers have the systems and processes in place to prevent a data breach.

This guide takes a deep dive into the PCI compliance requirements you need to follow from both an IT and business perspective. We'll talk about:

- What it takes to become PCI compliant
- The consequences of non-compliance
- How your ecommerce platform impacts compliance
- Why over 60,000 online stores choose BigCommerce to protect their sensitive customer data

12-Step PCI Requirements Checklist

Here are the 6 primary objectives and 12 basic requirements in PCI DSS 3.2.

OBJECTIVES	REQUIREMENTS	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data.	☐
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	☐
Protect Cardholder Data	3. Protect stored cardholder data.	☐
	4. Encrypt transmission of cardholder data across open, public networks.	☐
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs.	☐
	6. Develop and maintain secure systems and applications.	☐
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business justification.	☐
	8. Assign a unique ID to each person with computer access.	☐

OBJECTIVES	REQUIREMENTS	
Regularly Monitor and Test Networks	9. Restrict physical access to cardholder data.	☐
	10. Track and monitor all access to network resources and cardholder data.	☐
	11. Regularly test security systems and processes.	☐
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.	☐

Twelve requirements may not sound like much. In fact, a quick scan for PCI compliance documentation online will lead you to believe that PCI compliance is easy.

In reality, maintaining PCI compliance is extremely complex—especially for large enterprises. It actually means you need to comply with a total of 251 sub-requirements across the 12 requirements outlined in PCI DSS 3.2 to fully address the growing threats to customer payment information.

“Data breaches cost businesses an average of $150 per record.”

What if you don’t comply?

Failing to comply makes your business vulnerable to cyberattacks. That can lead to data breaches, which cost businesses an average of **$150 per record**. Penalties for non-compliance with PCI DSS are severe.

Although PCI is a set of industry rules, not a law, non-compliant merchants are penalized by their acquiring banks. Banks can fine you anywhere from $5,000 to $100,000 every month until all compliance issues are addressed. If problems aren't resolved, you could even have your ability to accept credit cards revoked.

A breach of cardholder data can be devastating to your business beyond your bank's penalties as well. You also risk:

- Damage to your reputation with customers, partners, and suppliers
- Possible civil litigation from breached customers
- Potentially going out of business

The bottom line is that you need to protect your customers' payment data before, during, and after purchase by detecting, preventing, and responding to cyberattacks. To do that, you need to take a deeper dive into the 12 requirements.

What you really need to know about the 12 requirements

If you're in charge of your company's PCI compliance, take a closer look at the **Requirements and Security Assessment Procedures for PCI DSS 3.2** to fully understand what it takes to maintain compliance.

If you aren't ready to dive in that deep yet, keep reading for a summary of each requirement along with actionable IT checklists.

Requirement 1

Install and maintain a firewall configuration to protect cardholder data.

Firewalls provide a first line of defense for your network, restricting outgoing and incoming traffic through rules your business sets up. It's best to start with a "block everything" firewall strategy and then add exceptions as needed.

Devices that connect to your cardholder data environment (CDE) remotely need to have a software firewall installed. PCI DSS requires you to document reasons for any communication allowed to or from your CDE.

Some businesses set up large, flat networks where every internal system can connect to everything else and there's only one firewall at the edge of the network. This approach makes securing your customers' payment card data more difficult because an attacker has access to every system once he gets inside of your network.

A better strategy is to implement segmentation within your network, creating secure payment zones that are firewalled off from the rest of your traffic. This ensures that your CDE only communicates with trusted sources and reduces your risks of a breach.

Regardless of the way you implement firewalls, you need to review logs every day to identify activity that indicates attempts to breach security. Review your firewall rules regularly and perform configuration tests at least every six months.

Requirement 1: IT Checklist

- [ ] Position firewalls to only allow necessary traffic to enter your CDE.
- [ ] Have a “deny all” rule for all other inbound and outbound traffic.
- [ ] Have dynamic packet filtering.
- [ ] Create a secure zone for any card data storage.
- [ ] Ensure all outbound connections from your CDE are explicitly authorized.
- [ ] Install a firewall between wireless networks and your CDE.
- [ ] Document all firewall policies and procedures, including business justification for each port or protocol allowed through firewalls.

Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters.

Devices such as POS systems and routers come with factory settings like default usernames and passwords that make installation and support easier, but also make it easy for hackers to breach.

Use configuration and hardening standards when setting up systems. Make sure passwords are changed every 90 days and that they contain at least seven numeric and alphabetic characters.

Configuration and hardening requirements apply to all systems, network devices, and applications you use to secure or process cardholder data.

- System hardening practices include:
- Disabling features and services you don't use
- Uninstalling applications you don't need
- Limiting systems to perform a single role
- Removing default accounts
- Changing default passwords

To secure your environment to meet PCI standards, understand where your credit card data is stored and transmitted. Document the flow of cardholder data through your network, making an inventory list of every application, device, and system it touches along the way. After you identify and document everything that needs to be secured, implement a process to consistently review your environment to discover vulnerabilities and threats as time goes on.

Requirement 2: IT Checklist

- [ ] Keep an inventory of all hardware and software used in the CDE.
- [ ] Assign a system administrator to be responsible for configuring system components.
- [ ] Implement a system configuration and hardening guide that covers all components of the CDE.
- [ ] Disable or uninstall any unnecessary services, programs, accounts, drivers, scripts, features, systems, and web servers, and document which ones are allowed.
- [ ] Change vendor-supplied default usernames and passwords.
- [ ] Document security policies and operation procedures for managing vendor defaults and other security settings.
- [ ] Use technologies such as VPN for web-based management and ensure all traffic is encrypted following current standards.
- [ ] Enable only one primary function per server.

Requirement 3

Protect stored cardholder data.

Stored payment card data must be encrypted using industry-accepted algorithms. Encryption keys must be protected as well. PCI compliance requires you to encrypt data once it's received, set timeframes to keep data, and have a documented procedure to delete unnecessary data.

It's important to understand what data you actually have, so you need to create and document a cardholder flow diagram that shows how payment card data moves throughout your company.

Find out which departments may receive or store cardholder data, and then build out your diagram considering:

- What devices you're using for transactions
- What happens to payment card data after a transaction
- When data is encrypted
- Whether you store card data before it's sent to the processor for approval
- How settlement occurs
- How data is authorized and returned by the processor
- Whether card data is backed up and encrypted on your system
- Whether your backup server is at a different location
- Where card data might be going or moved in processes not part of authorization and settlement

Using a payment card data discovery tool is the most effective way to find unencrypted data. After you locate all of it, review your policies and PCI DSS to determine what data you're allowed to keep.

Requirement 3: IT Checklist

- [ ] Document a data retention policy.
- [ ] Have employees acknowledge their training and understanding of the policy.
- [ ] Eliminate storage of sensitive authentication data after card authorization.
- [ ] Mask the primary account number on customer receipts.
- [ ] Understand guidelines for handling and storing cardholder data.
- [ ] Make sure primary account number storage is accessible by as few employees as possible, including limiting access to cryptographic keys, removable media, or hard copies of data.

Requirement 4

Encrypt transmission of cardholder data across open, public networks.

Identify where you send cardholder data and use encryption when you transmit cardholder data over open, public networks such as:

- Corporate offices
- Processors
- Backup servers
- Third parties that store or handle cardholder data
- Outsourced management of systems or infrastructure

The PCI Security Standards Council required businesses to transition from SSL (Secure Sockets Layer) and early versions of TLS (Transport Layer Security) to secure versions of TLS by June 30, 2018.

Contact your acquiring bank, terminal providers, gateways, and other vendors to find out if the devices and applications you use have this encryption protocol. If so, stop using these services and transition to providers, devices, and applications that use secure versions of TLS. Using these outdated technologies puts you at risk of a security breach.

Requirement 4: IT Checklist

- [ ] Review all locations, systems, and devices where cardholder data is transmitted to ensure you're using appropriate encryption to safeguard data over open, public networks.
- [ ] Verify encryption keys/certificates are valid and trusted.
- [ ] Continually check the latest encryption vulnerabilities and update them as needed.
- [ ] Have a policy to ensure you don't send unprotected cardholder data via end-user messaging technologies.
- [ ] Check with vendors to ensure supplied POS devices are appropriately encrypting data.
- [ ] Review and implement best practices, policies, and procedures for sending and receiving payment card data.
- [ ] Enable TLS whenever cardholder data is transmitted or received through web-based services.
- [ ] Prohibit the use of WEP, an unsecured wireless encryption standard.

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs.

Install anti-virus software on all systems that can be impacted by malware, as well as update it on a regular basis to detect and prevent known malware from infecting your systems. This applies to client-based configurations on servers as well as workstation installations. Being vigilant with regular anti-virus scanning proactively reduces the opportunity for hackers to gain access to your environment to steal cardholder data.

Requirement 5: IT Checklist

- [ ] Deploy anti-virus programs on commonly affected systems.
- [ ] Set anti-virus system to scan automatically to detect and remove malicious software.
- [ ] Maintain audit logs for review.
- [ ] Set anti-virus system to update automatically.
- [ ] Set up administrative access to ensure anti-virus can't be disabled or altered by users.
- [ ] Document malware procedures and review them with necessary staff.
- [ ] Examine system configurations and periodically evaluate malware threats to your system.

Requirement 6

Develop and maintain secure systems and applications.

Quickly implementing security updates is critical for protecting your sensitive data. To maintain compliance, PCI DSS requires merchants to deploy necessary patches within 30 days of release.

Secure all critical components in the card flow pathway, including:

- Operating systems
- Databases
- Application software
- Firewalls
- Internet browsers
- POS terminals

The more systems, computers, and apps your company has—including payment card applications and mobile devices—the more vulnerable you are to hackers. Scan all of these regularly to reveal vulnerabilities that cybercriminals can leverage to compromise your systems and steal cardholder data.

Have proper change control processes and procedures in place that:

- Separate test environments from production with proper control to enforce access rights
- Separate duties between personnel assigned to test environments and those assigned to production
- Keep production data from being used in test environments
- Remove all test data and accounts before a production environment becomes active
- Ensure changes:
  - *Have a documented explanation of what will be impacted by the change*
  - *Have documented approval by authorized parties*
  - *Undergo proper iterations of testing and QA before being released into production*
  - *Include a roll-back procedure in case the updates aren't properly implemented*

Requirement 6: IT Checklist

- [ ] Have a change management process.
- [ ] Have an update server.
- [ ] Have a process in place to keep up-to-date with the latest identified security vulnerabilities and their threat level.
- [ ] Install vendor-supplied security patches on all system components.
- [ ] Ensure all security updates are installed within one month of release.
- [ ] Set up a manual or automatic schedule to install the latest security patches for all system components.

Requirement 7

Restrict access to cardholder data by business need-to-know.

Only give access to payment card systems and data to people who need to know that information to perform the duties of their job. Create a role-based access control system with an up-to-date list of user roles that includes the definition of each role, data they can access, their current privilege level, and the privilege level needed to perform normal business responsibilities. User access and documentation applies to anyone who needs to access your systems, including everyone from normal office staff to contracted IT maintenance workers.

Requirement 7: IT Checklist

- [ ] Implement access controls on any systems where cardholder data is stored and handled.
- [ ] Have a written policy that details access to cardholder data based on defined job roles and privilege levels.
- [ ] Train employees on their specific access level.
- [ ] Configure access controls to only allow authorized parties and deny all others without prior approval or access.

Requirement 8

Assign a unique ID to each person with computer access.

Requiring complex passwords that aren't easy for hackers to crack is critical to safeguard cardholder data. Change passwords every 90 days and make sure they have at least seven characters including an upper- and lower-case letter, a number, and a special character. PCI DSS requires an account to be locked after six consecutive failed login attempts within a 30-minute period.

Since January 31, 2018, PCI DSS has required multi-factor authentication to secure remote access. Effective multi-factor authentication examples include:

- Requiring a remote user to enter their username and password, and then requiring them to enter a one-time password sent to them on their smartphone
- Requiring a remote user to enter their username and password, and then requiring them to use a unique dynamic number found on a RSA SecurID token

Requirement 8: IT Checklist

- [ ] Monitor all remote access accounts used by vendors, business partners, IT support personnel, etc. when the account is in use.
- [ ] Disable all remote access accounts when not in use.
- [ ] Enable accounts used for remote access only when they are needed.
- [ ] Implement a multi-factor authentication solution for all remote access sessions.

Requirement 9

Restrict physical access to cardholder data.

A comprehensive physical security policy that includes all of the processes and rules necessary for safeguarding your business—day and night—is crucial. This involves everything from keeping sensitive data and equipment secured in a locked area to requiring non-employees to wear visitor badges at all times.

Some physical security best practices:

- Have electronic access on doors
- Require passwords to access computers and mobile devices
- Encrypt your data or do not store data on these devices
- Ensure all workstations have an automated logout and use privacy monitors on computers
- Keep logs of who goes in and out of the office
- Keep track of devices that go in and out of the office
- Have an incident response plan for stolen equipment
- Train staff against social engineering
- Limit access to cardholder data through role-based access
- Encourage staff to report suspicious people and devices
- Monitor secure areas with video cameras and store the video logs for appropriate durations

PCI DSS requires you to control employee access to areas and devices where sensitive information is stored. Document:

- Who has access to secured environments and their business need
- What, when, where, and why devices are used
- A list of authorized device users
- Locations where the device is and is not allowed
- What applications can be accessed on the device

Businesses who use POS systems, PIN pads, and mobile devices are required to do three new things under PCI DSS 3.2:

- Maintain an up-to-date list of all devices
- Periodically inspect devices
- Provide staff awareness training

Requirement 9: IT Checklist

- [ ] Restrict access to any publicly accessible network jacks in the business.
- [ ] Keep physical media secure and maintain strict control over any media being moved within the building and outside of it.
- [ ] Keep media in a secure area with limited access and require management approval before the media is moved from its secure location.
- [ ] Use a secure courier when sending media through the mail so the location of the media can be tracked.
- [ ] Destroy media in a way that it cannot be reconstructed.
- [ ] Maintain a list of all devices used for processing and training all employees to inspect devices for evidence of tampering.
- [ ] Have training processes for verifying the identity of outside vendors wanting access to devices and processes for reporting suspicious behavior around devices.

Requirement 10

Track and monitor all access to network resources and cardholder data.

PCI DSS 3.2 requires you to implement a process to quickly detect and respond to security failures.

Define an incident response plan that fixes the problem and also identifies root causes and risks, documents lessons learned, and implements changes to prevent a breach from happening in the future.

Have a log monitoring system in place. Log monitoring systems oversee your network activity, alert you about suspicious activity, inspect system events, and store user actions that occur inside your systems. Log alerts act as a red flag when a breach has occurred, so regularly reviewing logs enables you to quickly identify and stop malicious attacks. In fact, PCI DSS requires you to review your logs every day to search for anomalies, errors, and suspicious activity.

Define your log management strategy:

- Decide when and how to generate logs
- Set up a team to review suspicious alerts
- Assign an employee you trust to review logs on a daily basis
- Secure stored logs so they aren't altered by hackers
- Define rules for creating alerts
- Store logs for at least one year and have three months readily available

Regular log monitoring enables you to have a faster response time to attacks and defend against threats.

Requirement 10: IT Checklist

- [ ] Track every action taken by someone with administrative privileges, failed login attempts, and changes to accounts in audit logs.
- [ ] Have the ability to identify a user, the date and time of the event, the type of event, whether the event was a success or failure, where the event originated from, and the name of the impacted data or system component.
- [ ] Create processes and procedures to review logs and security events daily, as well as review system components defined by your risk management strategy.
- [ ] Have a process to respond to anomalies or exceptions in logs.
- [ ] Keep all audit log records for at least one year and keep logs for the most recent three months readily available for analysis.

Requirement 11

Regularly test security systems and processes.

PCI DSS requires you to perform vulnerability scans and penetration tests to identify how susceptible your systems are to an attack.

A vulnerability scan is an automated, high-level test that scans both internal and external environments for vulnerabilities. You perform external vulnerability scans outside of your network to identify known weaknesses in network structures. Internal vulnerability scans are performed within your network to examine other hosts on the same network to find internal vulnerabilities.

Perform a formal penetration test at least yearly and whenever you make a large infrastructure change to determine whether it added any new vulnerabilities. The main difference between a vulnerability scan and a penetration test is that a vulnerability scan is automated, whereas a live person performs a penetration test to dig deeper into the vulnerabilities to identify the root causes that allow access to your sensitive data.

Conduct different types of penetration tests:

- **Network penetration test:** Finds security issues with the design, implementation, and maintenance of servers, network services, and workstations.
- **Segmentation test:** Discovers whether a cybercriminal can access your network because of a misconfigured firewall.
- **Application penetration test:** Finds security issues as a result of insecure development, design, coding, and publishing of software.
- **Wireless penetration test:** Discovers whether wireless infrastructure has been misconfigured and whether there are unauthorized access points.
- **Social engineering test:** Finds employees that don't properly follow processes and enable potentially dangerous threats to access your network, such as clicking on malicious emails or allowing unauthorized people into the building.

Requirement 11: IT Checklist

- [ ] Run quarterly internal vulnerability scans using a qualified internal resource or external third-party.
- [ ] Run quarterly external vulnerability scans using a PCI-approved scanning vendor (ASV).
- [ ] Use a qualified resource to run internal and external scans after any major change to your network.
- [ ] Configure change-detection tools to alert you to unauthorized modification of critical content files, system files, or configuration files.
- [ ] Configure tools to perform critical file comparisons at least once a week.
- [ ] Have a process to respond to alerts generated by the change-detection tool.
- [ ] Run a quarterly scan on wireless access points and develop a plan to respond to the detection of unauthorized wireless access points.
- [ ] Perform penetration tests to confirm segmentation is operational and isolates systems in the CDE from all other systems.

Requirement 12

Maintain a policy that addresses information security for all personnel.

Document all security measures your business takes to protect cardholder data. PCI DSS requires you to keep a list of all third-party service providers, PCI requirements the service providers handle, and PCI requirements you have to meet.

Your security policy should include documentation for:

- Policies and procedures
- Third-party service provider agreements
- Incident response plans
- Employee manuals

PCI DSS 3.2 requires you to perform a risk assessment at least once a year to identify critical assets, vulnerabilities, risks, and threats. Conduct regular training with employees to keep them up-to-date with your security policies and to review best practices for safeguarding cardholder data.

Requirement 12: IT Checklist

- [ ] Develop written compliance and security policies.
- [ ] Ensure every employee working in the CDE completes annual security awareness training.
- [ ] Create a company policy documenting all critical devices and services within the CDE, including laptops, tablets, remote access, wireless access, and email/Internet usage.
- [ ] Develop a comprehensive description of each employee's role in the CDE, and document acceptable uses and storage of all technologies.
- [ ] Create an incident response plan in the event cardholder data is compromised.
- [ ] Create and update a current list of third-party service providers.
- [ ] Annually document a policy for engaging with third-party providers, obtain a written agreement acknowledging responsibility for the cardholder data they possess, and have a process for engaging new providers.

Simplify PCI Compliance

It's pretty clear that achieving and maintaining PCI compliance isn't an easy task. Doing it on your own requires a massive amount of time, money, and personnel.

The stakes are high when your customers' sensitive data—and your business itself—are on the line. Partnering with the right company can help you remain compliant without breaking the bank.

How your ecommerce software affects PCI compliance

Your choice of ecommerce software can dramatically impact your PCI compliance risks, responsibilities, and costs. Let's examine three approaches you can take to ecommerce platforms:

1. COMMERCIAL SOFTWARE

This option is the most expensive because it requires you to purchase and maintain your own hardware, as well as pay for a commercial software license and annual support. Unless the software is PCI compliant out-of-the-box, the vendor provides free PCI compliance support, or you have in-house PCI experts—all of which are unlikely—achieving compliance with this approach can be extremely costly.

2. ON-PREMISE, OPEN SOURCE SOFTWARE

This approach is less expensive than the first option, but the risk is even higher. You still maintain your own hardware, but you avoid paying software license fees. It's your responsibility to assemble, install, and fine-tune your own software, and you're 100% responsible for PCI compliance. There's no vendor to rely on for assistance. Unless you're willing to buy and maintain on-premise hardware, pay in-house experts to maintain the software, and pay a team of in-house PCI experts to hold the many meetings needed to create all of the required PCI documentation, this probably isn't the right approach either.

3. HOSTED SOFTWARE AS A SERVICE (SAAS)

A SaaS ecommerce solution is the best approach for most enterprises because it combines the lowest cost with the lowest risk. The software is provided as a service and is accessed online, and the hardware is maintained in a secure data center. Using a hosted ecommerce service enables you to:

- Pay a monthly fee to use the software
- Save money on hardware, software licenses, staff, and support
- Save the resources you would have needed to dedicate to PCI compliance activities
- Let the PCI experts at the SaaS ecommerce company handle PCI compliance with minimal effort from you

Why enterprises choose BigCommerce

You've likely followed the many high-profile data breaches large enterprises have experienced in recent years. In the first half of last year, there were 3,800 publicly disclosed data breaches exposing **4.1 billion compromised record**s. When you consider that the global average cost of a data breach is **$3.92 million**, online sellers have a huge incentive to protect customers' sensitive data.

One of the best ways to set your business apart from your competitors is to make it measurably more secure. After all, if you don't meet the security requirements of your customers—let alone PCI DSS 3.2—you risk losing business to competitors who view security as a high priority.

BigCommerce is committed to delivering PCI DSS compliant ecommerce solutions that make your business more secure. As a **SaaS ecommerce platform** and certified PCI DSS 3.2 Level 1 Service Provider, BigCommerce bears the burden of PCI compliance for your business. This protects you from payment card data breaches and eliminates the massive cost and hassle of managing compliance yourself.

We handle millions of transactions for more than 60,000 brands every day in a safe and reliable environment. Our advanced ecommerce technology, PCI experts, and payment processing partners ensure that you are always PCI compliant.

With BigCommerce, you:

- Don't need to worry about updates or upgrades – we handle all patches and bug fixes
- Never store cardholder data on your own systems – there's no risk.
- Are never vulnerable to payment data breaches – avoid the negative PR that comes with a breach.
- Never lose your ability to collect payments online – maintain credibility with banks and credit card processors.
- Don't pay for software licenses, hardware, and servers – you just pay a monthly fee to use the platform.
- Have a lower total cost of ownership – our SaaS ecommerce solution is 75% less expensive than on-premise enterprise ecommerce solutions like Magento.
- Don't have to worry about downtime costs – we have 99.99% uptime compared to 99.5% for the ecommerce industry as a whole.
- Never pay for support costs – we handle all maintenance and provide 24x7 customer support.
- Build customer trust – your reputation as a secure seller can lead to higher sales.

It's no wonder that leading enterprises choose BigCommerce when you consider the lower costs, less risks, and fewer PCI hassles they have to deal with on their own. Our team of PCI experts make sure you adhere to the 12 PCI DSS 3.2 compliance requirements so you can focus on serving your customers and growing your business.

With 251 sub-requirements to follow, numerous policies and procedures to develop, and dozens of documents to create and report, achieving and maintaining PCI compliance is a complicated process. The consequences of getting it wrong can be devastating for your business, so your best bet is to trust PCI compliance to ecommerce experts.