In a time where phishing attempts and cyberattacks are a widespread concern, you need a clear roadmap for protecting your business from malicious cyber criminals. For businesses dealing with cardholder data, the roadmap has already been laid down in the form of Payment Card Industry – Data Security Standard (PCI-DSS). Any business that needs to process their payment information online must pursue PCI compliance standard to ensure that its following best practices of customer data security and protection. Created by the PCI – Security Standards Council (PCI-SSC), the standard works towards increasing protection and controls around cardholder data while reducing the risk of credit card fraud at the same time.

If your business is PCI compliant, it shows a major progress in your efforts towards preventing data breaches and cyber-attacks. For organizations that process payments online, PCI DSS goes completely in their interest. To put it easily, regardless of its size, any business that processes, stores or transmits [cardholder](http://www.cardzgroup.com/%20or%20http:/www.cardzgroup.com/ContactSmartCard.html) data and related sensitive information must ensure PCI compliance. This pretty much applies to all Ecommerce businesses. However, the level of adherence varies according to the number of credit card transactions every business processes. A company that suffers a breach while being non-compliant or not fully compliant can end up paying fines to the PCI SSC, hence adding further financial repercussions to the loss resulting from the breach. Thus, PCI compliance is a worthwhile pursuit for businesses that seek to protect their reputation and customer data.

For any business to become PCI-DSS compliant, there are five simple ways that it must follow:

1. **Determine Your PCI Level and Scope**

Merchants that annually process over six million transactions are considered level one while those between one and six million are designated level two. Level three merchants are those with 20,000 to one million transactions per year. Any transactions lesser than this are at level four. Each level has to adhere to its requirements pertaining to PCI-DSS.

Once you determine your level, you also need to determine the scope of your compliance. Scope involves any process, person or component that stores, processes or transmits cardholder data. Components that may be a part of your scope include servers, networking devices, routers, computing devices and applications. Determining scope is important to know which entities handle your credit card data. It’s not possible to protect what you don’t know and likewise impossible to secure it.

Creating a payment card data flow diagram for in-scope entities can ensure that you don’t miss out on anything. This is why you should start documenting the process from the very first step in order to make it easy for employees to understand what was done, how it was done and what still needs to be done. Moreover, whenever there are any changes in your business’s security, document the changes. It’s also a good idea to review the documentation (at least quarterly) to ensure that no errors are made.

1. **Complete Self-Assessment Questionnaire**

Self-assessment questionnaires are available at the [PCI SSC website](https://www.pcisecuritystandards.org/pci_security/completing_self_assessment). There are different questionnaires applicable to different businesses, but each has a series of yes or no questions that help you determine how closely you meet the requirements of PCI DSS. Any answer in “No” indicates a red flag and requires appropriate action. Very commonly, businesses lag behind in compliance in the areas of vulnerable authentication credentials, outdated security protocols and failed SSL certificate verification.

Getting your employees to get CompTIA’s [CASP+ certification](https://www.comptia.jp/pdf/casp_cas-003_objectives.pdf) equips them with advanced-level security knowledge and technical skills and ensures that they are able to optimally self-assess their organization’s security position.

1. **Create and Maintain a Secure Network**

For this step, small businesses will need to find an information technology contractor they can trust. With little technical expertise, it’s favorable to leave the important task of network security and firewalls to those who specialize in it. PCI compliance requires businesses to use systems that stop unauthorized access by untrusted factors. Once you implement your firewall, develop a robust password program, change default passwords and continue to change them at regular intervals. Always keep your firewall operational and updated. No employee should ever have a reason to disable it.

As a large organization with an IT department, you will need trained and certified employees who hold the responsibility to ensure network security. Among other things, CompTIA’s [Security+ certification](https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf) exam measures your ability to identify attacks, threats and vulnerabilities and to install and configure software and hardware-based network components to support organizational security.

1. **Train Your Staff**

Are you aware that [60 percent of data breaches](http://blogs.wsj.com/cio/2015/02/26/the-weakest-link-is-your-strongest-security-asset/) are a result of negligence by corporate partners and employees? Employees are often the weakest security link. Still, most of the businesses do not consider spending enough time to train them properly for security.

The best way to train your employees is to create customized programs for individual roles of employees. For instance, a front-desk officer will require different training than an operational manager. Since humans tend to forget easily, and the best way to retain information is through repetition, it’s always better to train monthly instead of annually.

Our [CASP+ certification](https://www.comptia.jp/pdf/casp_cas-003_objectives.pdf) exam is designed to ensure that your employees handling critical data are equipped to understand, retain, compare and contrast security policies and procedures based on organizational requirements.

1. **Hire a Security Professional**

Lastly, consider working with a security expert or a Qualified Security Assessor (QSA) to ensure complete PCI compliance. QSA’s are intensively trained to understand every detailed requirement of data security and PCI DSS, and have the required technical expertise to guide you through your entire PCI compliance process. If you are a small business, you may not need a PCI DSS audit, but would still need to consult with a PCI professional to walk you through your compliance path.

Your road to PCI compliance may be complex, but it is worth the travel if you want to guard customer data, avoid reputational damage and future-proof your business.