
Complior
THE ULTIMATE GUIDE TO
PCI DSS CLOUD HOSTING

INTRO

You collect payment from your customers online and you know it's your company's responsibility to keep that information secure, confidential and from getting hacked and released into the world of the Internet.
It's your reputation, your brand and your customer's trust all on the line.
So what exactly do you need to do for your business to both meet customer's expectations, the guidelines and standards set out by governing bodies?
Do you need to hire an expert in-house or is there a reliable service you can partner with to outsource to comply?

Below we outline the ultimate guide for all you need to know about the Payment Card Industry Data Security Standard (otherwise referred to as PCI DSS) and options for your business.

IN THIS GUIDE:

SHOULD YOU OUTSOURCE?

What exactly is PCI DSS?

The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard for entities that handle payment card data from the major card companies including Visa, MasterCard, American Express, Discovery and JCB. The standard was created to increase controls around cardholder data to reduce credit card fraud and maintain payment security.

Basically if you or your company provide goods or services to clients and collect payment, which most businesses do to stay operational, you must protect, by law, the personal and financial information of those clients to a certain standard.

Cyber security is one of the top threats for businesses today whether you are a small ecommerce site or international conglomerate. It is your company's responsibility to ensure a high level of security; especially when collecting and storing sensitive information like payment data and personal customer information. The Internet is flowing with personal information and in 2018 alone cybercrime cost the global economy over 600 billion dollars! (McAfee)

So what's the solution?

PCI DSS (Payment Card Industry Data Security Standard) is a security standard designed to protect payment data, and every company that handles credit card data has to be PCI compliant. If your company does not meet the standard, you risk fines, a potential loss in revenue and the worst, harm to your reputation, which in today's online Google reviews & Facebook recommendations world can shatter businesses.

One thing to note is that compliance does not come cheap. The complexity, effort and cost required to ensure the safeguarding of sensitive data has led to an increasing number of companies looking for solutions to simplify compliance.

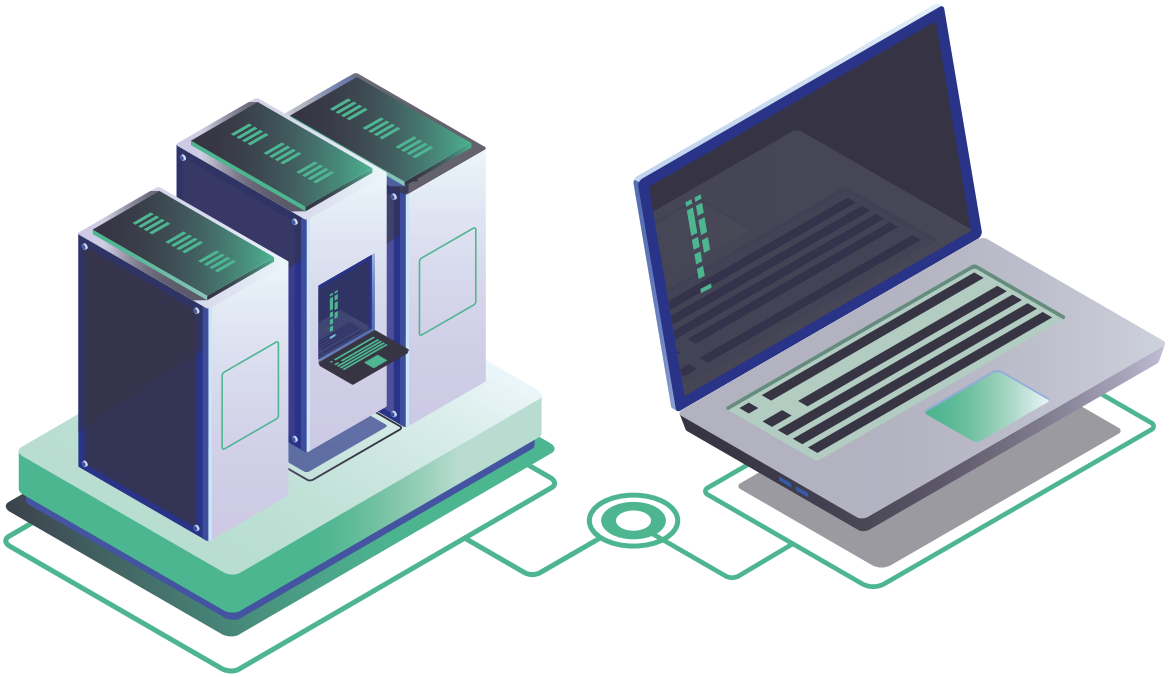
Don't underestimate the importance of PCI scope and accountability for your organization. Understanding the PCI DSS requirements and the benefits of outsourcing compliance hosting can save you and your company many headaches and potential legal battles down the road.

There are options to outsource your IT environment to a PCI DSS certified cloud-hosting provider, knowing your customers and business are protected while you focus on scaling your business and achieving your goals and targets. Trusting this to experts can be especially beneficial to small merchants who have limited resources.

Outsourcing hosting to a PCI DSS certified hosting provider

When you have to comply with laws and regulations like PCI DSS, GDPR and ISO, it is natural to seek efficient solutions to fulfill the requirements. Solutions that simplify scope, simplify security, and simplify compliance without compromising the security level of your organization.

Outsourcing operations to a PCI DSS certified cloud provider essentially means handing over some of the responsibility for PCI DSS compliance to someone else. It also means that you, through your hosting provider, automatically reach some of the requirements in PCI DSS. It should be noted that moving to the cloud and choosing a PCI DSS certified cloud provider doesn't automatically make you PCI DSS compliant. But it does significantly simplify compliance.



PCI DSS CLOUD HOSTING

How does it work?

Outsourcing operations to a third party means that you share responsibility for reaching the requirements in PCI DSS. Your hosting provider fulfills some requirements, and your company has to fulfill others. The PCI DSS requirements focus on 3 areas: technology, processes and people.

Your provider provides the cloud infrastructure and is responsible for most of the technology-related requirements. You are responsible for the requirements related to people and processes.

When using a third party PCI DSS certified service or hosting platform, your company will have to submit a responsibility matrix to the QSA. The responsibility matrix details who is responsible for what PCI requirements

What assets do you need from potential service providers?

Attestation of Compliance

The AOC (Attestation for Compliance) is a form that shows the results of the PCI DSS audit, signed by both the company and the PCI QSA. An AOC is the certificate that offers proof that the service provider or merchant is PCI compliant. If you're a merchant, the service provider's AOC shows that you fulfill some of the requirements in PCI DSS. An AOC is considered to be 'Third Party Proof' by the PCI Council.

Responsibility Matrix

A responsibility matrix is a list of requirements and indicates which requirements are the responsibilities of the service provider, the merchant, - or two service providers - and which are shared between them. A responsibility matrix is a great way to get an overview as to how much PCI compliance is simplified when choosing to place your environment in a PCI DSS certified cloud.

The responsibility matrix should for each requirement specify:

- How the service provider performs, manages and maintains the required control.
- How the control is implemented, and what the supporting processes are.
- How the service provider will showcase evidence as needed that controls are met.

It can look something like this

Requirements	Description	Responsibility		Main responsibility
		Complior	The customer	
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that exisiting log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Is responsible for the Hosted environment.	Is responsible for The Customer's applications	Complior
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Is responsible for the Hosted environment and The Customer's applications	Is responsible for providing instructions for the application log review	Complior
10.6.1	Review the following at least daily: * All security events * Logs of all system components that store, processor transmit CHD and/or SAD * Logs of all critical system components	Is responsible for the Hosted environment and The Customer's applications	Is responsible for providing instructions for the application log review	Complior

This allows everyone involved to understand their role, undertake and deliver on their responsibility and continually keep your organization PCI DSS certified.

The 5 benefits of outsourcing to a PCI certified hosting provider

It requires a lot of effort to reach the requirements in PCI DSS. Outsourcing allows you to simplify your compliance efforts, saving you a lot on resources. Besides fulfilling the majority of requirements, there are other benefits of choosing a PCI DSS certified cloud platform:

1. Cost Effective

One of the biggest motivations for any business decision is cost. You want the best you can get for the lowest price possible. The case is the same with PCI DSS. Using a third party provider for PCI Compliance and security can save your business money.

Investing in an outsourced service allows for high levels of protection to be achieved without enormous investment in resources like staff and infrastructure. These cost savings can especially make a huge difference for small companies and startups.

2. Dedicated security specialists

Running a business is a lot like juggling.

You juggle the different components that make up your business: products, profitability, costs, staff, etc. Add compliance and security to that and balls begin to drop.

One of the major benefits of outsourcing to a PCI DSS certified cloud provider is that you gain access to compliance and security experts. Those who know the ins and outs of PCI DSS – this knowledge is part of the package. You can stay up to date with the latest in the industry, including PCI DSS updates, innovative new technology and the latest tactics used by cyber criminals targeting the payment industry.

Having industry specialists on hand can also help you better identify vulnerabilities and weaknesses as well as improve incident response capabilities. This allows for a quick response to security and compliance issues.

3. Support around the clock

Protecting sensitive data is a 24/7/365 job. Outsourcing IT-operations to a hosting provider means that you get support around the clock, and can respond to threats and incidents immediately. When your network is monitored continuously you significantly reduce potential downtime and its impact on your clients.

4. Stamp of security

By choosing a PCI DSS certified provider, you can be sure that there is a high level of security where your data resides. The third party provider goes through the PCI DSS audit process every year, and has to have their security tested each quarter.

Using a PCI DSS certified cloud solution validates your security posture as a company that prioritizes safeguarding payment data. This will improve trust among your customers, and can be a powerful tool in your marketing efforts. In fact many customers are now informing themselves prior to selecting where and to whom they provide credit card data, and actively seek out this stamp of security.

5. Easier to scale

The goal for businesses is to grow, right? Cloud solutions are scalable in nature, and the same goes for PCI DSS-certified cloud hosting. You don't have to invest in your own hardware, the hosting provider handles that for you. The solution is scalable as you grow, without affecting security.

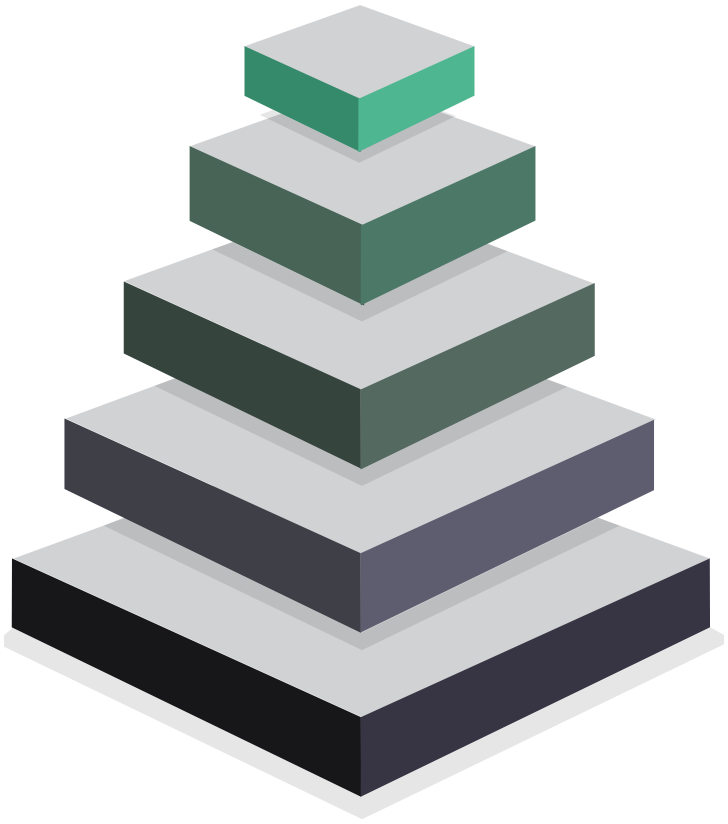
ARE YOU PROTECTING YOUR CLIENT DATA SECURELY ENOUGH?

Understanding Levels of PCI DSS Compliance

How rigorous is the certification process?

If you're a small to medium sized business do you have to meet as many requirements and jump through as many hoops as a large enterprise? The answer is yes and no.

There are many benefits to partnering with a PCI DSS cloud hosting provider like Complior. In the last chapter, we outlined the 5 Benefits of Outsourcing including costs, staying up-to-date and scalability. Understanding what the PCI DSS certification process entails is outlined in this post below to help you grasp what's in store as your company works to become PCI DSS compliant.



PCI DSS Requirements[1]:

PCI DSS outlines technical and operational requirements for those who in any way store, process and/or transmit payment card data. PCI DSS has 12 main requirements and over 300 sub-requirements. The standard is ever-developing to reflect the payment industry, and updated versions are released regularly.

The PCI DSS requirements are related to the technology, people and processes surrounding payment card data. This is to ensure a high level of security for everything involved in the process of handling payment card data.

Build and Maintain a Secure Network

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. Use 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 need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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 employees and contractors

*https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

PCI DSS Levels:

The first thing you need to know is that the PCI DSS certification process can be very different between businesses. This is dependent on how many transactions a company processes per year. Below we have outlined the different levels of PCI DSS compliance for merchants and service providers so you can get an understanding based on how many transactions your business currently processes annually.

Merchant provider levels of PCI Compliance:

Level 1	6 million or more Visa and/or MasterCard transactions processed per year.
Level 2	1-6 million Visa and/or MasterCard transactions processed per year.
Level 3	20,000 to 1 million Visa and/or MasterCard e-commerce transactions processed per year.
Level 4	Fewer than 20,000 online transactions a year or up to 1 million regular transactions per year.

Service provider levels of PCI compliance:

Level 1	Store, process, or transmit more than 300,000 credit card transactions annually.
Level 2	Store, process, or transmit less than 300,000 credit card transactions annually.

Note that a service provider is directly involved in the payment process as a third party. Service providers store and/or transmit payment data on behalf of other companies. Some examples are hosting providers and managed service providers.

PCI DSS Certification:

The PCI compliance levels are used to determine the amount of assessment and security validation required for the merchant or service provider to obtain a PCI DSS certification.

Based on the type of provider your business is and the number of annual transactions there are, this is what is expected during the certification process for each level.

	Merchant Providers:	Service Providers:
Level 1	1. Undergo annual on-site security assessments. 2. Undergo quarterly network scans by an ASV. 3. Submit an annual report on compliance (ROC) written by a QSA(Quality Security Assessor).	1. Undergo annual on-site security assessments. 2. Undergo quarterly network scans by an ASV. 3.Submit an annual report on compliance (ROC) written by a QSA (Quality Security Assessor). 4. Undergo penetration tests.Undergo internal scans. 5. Submit an Attestation of Compliance Form (AOC).
Level 2	1. Fill applicable Self Assessment Questionnaires (SAQ) annually. 2. Undergo quarterly network scans by an ASV.	1. Fill out the Self Assessment Questionnaire D (SAQ) annually. 2. Undergo quarterly network scans by an ASV. 3. Undergo penetration tests. 4. Undergo internal scans. 5. Submit an Attestation of Compliance Form (AOC).
Level 3	1. Fill applicable Self Assessment Questionnaires (SAQ) annually. 2. Undergo quarterly network scans by an ASV.	
Level 4	1. Fill applicable Self Assessment Questionnaires (SAQ) annually. 2. Undergo quarterly network scans by an ASV.	

It's worthwhile mentioning that since Level 1 companies process the most transactions per year, it is natural that these companies also have to fulfill the strictest PCI requirements on security.

Armed with this basic understanding of what PCI DSS is all about, the level of detail and significance it plays in the role of business today and how prudent it is to ensure you comply, are you ready to simplify your life and trust the certification process to PCI DSS experts?

Contact us for a free consultation and get started right away.

Complior