UNDERSTANDING PCI COMPLIANT DESKTOPS

How to avoid “PCI Compliance LITE” solutions

Some virtual desktop and desktop as a service (DaaS) providers offer PCI compliant solutions, but under the surface you may be getting minimal coverage that leaves you responsible for the majority of compliance requirements.

Understanding what’s required to support PCI DSS compliant virtual desktops and the division of responsibilities will have a big impact on the effectiveness, resources and financial implications of your PCI compliant solution.

DIZZION

UNDERSTANDING PCI COMPLIANT DESKTOPS

How to avoid “PCI Compliance LITE” solutions

For any organization that accepts, transmits or processes payment card data, Payment Card Industry Data Security Standard (PCI DSS) compliance is a critical component of doing business and protecting highly sensitive consumer information.

Created by the Payment Card Industry Security Standards Council, PCI compliance is divided into levels based on the amount of credit card transactions an organization transmits or processes annually. All organizations that fall under PCI requirements must have a specific set of security standards and controls in place.

Although the Payment Card Industry Security Standards Council is a private regulatory body, you cannot “opt out” or ignore PCI compliance. It’s also unwise to treat this requirement as simply a “check the box,” “bare minimum” task. Not only does this potentially leave customer data at risk, it can also have dire financial ramifications. Poor or non-compliance can lead to fines of up to $100,000 per month. This fine is levied by the payment brands of the Payment Card Industry Security Standards Council against banks and is often passed along to the merchant in violation. As further penalty, banks often freeze corporate bank accounts, terminate relationships with non-compliant organizations or increase transaction fees as a result of non-compliance. Beyond financial relationships, data breaches also often result in plummeting stock prices and consumer mistrust, which can lead to even greater financial impacts.

PCI compliance can clearly have a large effect on business. It’s also difficult to achieve and maintain compliance because of regularly updated standards (we’re now on PCI DSS 3.2) and an increasingly threatening cybersecurity landscape. To combat these challenges, companies often turn to solution providers for help meeting PCI DSS requirements. Unfortunately, many solutions and vendors – including VDI and DaaS providers – only offer low level support with their PCI compliant products. The key to finding a vendor that offers truly compliant desktops is to understand what’s involved in PCI DSS compliance and what to look for when vetting potential providers.

PCI COMPLIANCE RESPONSIBILITIES MATRIX

The PCI DSS outlines specific controls within 12 requirement categories that any organization that handles payment card information must comply with in order to be PCI compliant.

This checklist outlines those control sections and gives you a useful way of tracking responsibility to better evaluate PCI compliant desktop services.

DOWNLOAD ⟶

Brief PCI DSS Overview

There are 12 PCI DSS requirements that cover technical and operational aspects regarding how payment card data is handled:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system password and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
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
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

Each category includes a subset of specific requirements, resulting in nearly 1,000 controls that need to be addressed in order to be deemed compliant. Examples of individual controls include:

Control 1.1.7 - Requirement to review firewall and router rule sets at least every six months

Control 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Control 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

PCI DSS Compliance has more than 240 control sections containing over 800 controls.

When partnering with a virtual desktop provider, some of these controls fall squarely in their purview, some need to remain the client's responsibility and some will be shared. It's this division of responsibility that leaves some organizations with less compliance coverage than expected when purchasing a compliant virtual desktop solution. The shared responsibilities in particular are a source of complexity, misunderstanding and misaligned expectations in many partnerships.

Why Many DaaS Solutions Are "PCI Compliant LITE" … or Not Compliant at All

Whether you're looking into fully managed desktop as a service or an infrastructure as a service vendor hosted on a public cloud, you will find an increasing number of service providers that claim PCI compliance. There are two potential pitfalls to watch for in this situation:

1. The service provider is PCI complaint, but the specific solution or product you're purchasing does not have that designation.
2. The service provider covers very limited elements of PCI compliance, leaving you to fulfill the rest of the controls and requirements. This commonly takes the form of the provider's physical location being PCI compliant, but how the solution is implemented and everything that happens within the solution is not covered.

Scenario 1: Compliant Provider But Not a Compliant Solution

In this first scenario, the solution, service or product being offered is not PCI compliant. The service provider itself may meet compliance standards for their own needs and any work they do handling PCI, but the solution hasn't been audited and verified as compliant. There's no guarantee or documentation that the solution directly addresses or meets any of the controls required for a compliance. Just because a service provider is PCI compliant does not mean any of their services, solutions or products are also compliant unless those specific pieces have been individually audited and verified.

This means that you remain 100% responsible for PCI compliance, including all auditing and ensuring all controls are met. The service provider's compliance may be of limited help, but this shouldn't be considered a PCI compliant desktop solution and cannot be relied on to fulfill your compliance requirements. Essentially, any controls the solution fulfills are incidental and you're left to uncover, audit and document those – you can't trust that they're there because the solution provider has made no promise that they are.

The division of responsibility leaves some organizations with less compliance coverage than expected when purchasing a compliant virtual desktop solution.

Shared responsibilities in particular are a source of complexity, misunderstanding and misaligned expectations in many partnerships.

This can be confusing for decision makers as it appears that PCI compliance is in order and can result in ill-informed decisions that don't meet requirements or expectations. Offering PCI compliant virtual desktops is a big undertaking and any solution that has met this level of scrutiny will likely prominently advertise its status directly in line with the compliant product. Be cautious if the only mention of PCI compliance is buried on insignificant webpages rather than product pages. If PCI compliance is an important aspect of your outsourced virtual desktop initiative, specifically seek out DaaS providers that advertise PCI compliant desktops.

Scenario 2: PCI Compliance Lite

The second situation is a bit trickier to untangle. In this case, the solution (or portions of the solution) is technically PCI compliant but upon further inspection still leaves the customer with the majority of the responsibilities and controls associated with achieving and maintaining compliance. For organizations looking for an outsourced PCI compliant desktop solution that will make it easier to meet compliance requirements, these solutions leave much to be desired.

These partially compliant solutions typically have PCI controls in place at the data center level – arguably the easiest place to implement controls and likely something the provider needs for their own compliance. As you move deeper into the solution, however, controls quickly shift from the vendor's responsibility and become either a shared ownership or entirely in the hands of the customer. How the solution is implemented and used can thus have a major impact on compliance – and you're solely responsible for those aspects. Essentially, you're responsible for many of the points where PCI compliance can most easily break down. In this scenario, the solution is compliant on the surface, but adds very little value or protection in terms of practical compliance and everyday security and management duties.

Teams looking for a PCI compliant virtual desktop solution to ease the in-house compliance burden and add a level of protection to endpoints will find that choosing a weak or limited solution will not fulfill expectations or needs. Companies with limited in-house compliance expertise can turn to a good solution and service provider for guidance and assistance in achieving PCI compliance, but only if you select a robust solution and not one that offers bare bones compliance assistance.

What to Look for In a Compliant Solution

One of the easiest ways to assess whether a DaaS or outsourced VDI solution is PCI compliant is to ask if the specific solution, service or product you're vetting has been audited and verified by an independent PCI Qualified Security Assessor (QSA) and when the solution was most recently audited. If the answer is no, or not within the past 12 months, look for another DaaS provider as this vendor isn't committed to offering a truly compliant solution.

Once you've verified that the solution is PCI compliant (to guard against Scenario 1), ask to see a responsibilities matrix or RACI which details whether the service provider or the client is Responsible, Accountable, Consulted or Informed for each control (to guard against falling victim to Scenario 2). Any service provider offering a PCI compliant solution is required to provide some form of responsibilities matrix or RACI.

This document is a line by line delineation of PCI controls and clearly denotes if the responsibility for each control (and sub-control) belongs to the vendor, customer or is shared. It should include all 12 sections of PCI compliance and all 240+ control sections to give you a full understanding of ownership and product scope. Anything not specifically assigned to the vendor is the responsibility of the customer, regardless if it's associated with or controlled by the product or service.

Shared responsibilities are an area to pay close attention to. Some controls will naturally fall into this category as specific aspects (like access management) may be determined by both the vendor (for their team) and the customer (for your team). However, if a control could feasibly fall under the purview of both the solution and the customer – such as encryption and access methods or multi factor authentication – but is the sole responsibility of the customer, then the solution may not be helping you attain compliance as much as you planned since you will still carry the majority of responsibility. Carefully reviewing and understanding the vendor-provided responsibility matrix will help you determine if the solution will meet your required level of PCI support or if this solution is a textbook example of the second pitfall outlined above.

In addition to the responsibilities matrix, you can also inquire about an Attestation of Compliance (AOC). This document is further verification of the vendor's compliance status and should be completed by a QSA or third party auditor. It's important that vendors possess and can supply an AOC from an auditor to ensure independent validity and level appropriateness of their PCI compliant solution. Some organizations can also supply a Report on Compliance (ROC), however, a ROC alone should not be taken as proof of compliance. Instead, an AOC coupled with a responsibilities matrix should be provided.

Dizzion takes responsibility for more than 100 PCI control sections. Other "big box" desktop as a service and VDI providers that offer a compliant solution take sole responsibility for, on average, fewer than 25 sections.

Any service provider offering a PCI compliant solution is required to provide some form of responsibilities matrix or RACI.

Compliance is Complicated — Don't Increase Your Headache

Compliance is complicated and is costly to manage entirely in-house. Finding PCI compliant services and solutions eases much of the burden as it allows organizations to rely on experts and independently verified solutions to handle many of the required controls. To get the full benefits, however, it's important to find a service provider that doesn't offer a bare bones, check the box "compliant" service simply to say they do.

Have internal discussions with the IT, security and compliance teams to best understand the challenges you're trying to solve for, the current and future risk landscape, and how much compliance responsibility you expect a virtual desktop vendor to take on. Choosing a solution because it will help with IT needs and compliance only to find out that the compliance piece is lacking will leave team members bitter and with larger workloads. Ensuring everyone is on the same page regarding requirements, expectations and potential ramifications will help you better define the exact solution needed and find an appropriate PCI compliant virtual desktop vendor.

ABOUT DIZZION

Established in 2011, Dizzion, Inc. is a global provider of end-user computing services, including cloud-delivered Desktops as a Service (DaaS), paired with complementary offerings like secure endpoints, application delivery and storage. The company is delivering the next generation of virtual desktop solutions to meet the demands of a remote global workforce in industries with stringent security and compliance needs, including business process outsourcing, financial services, healthcare and insurance. Dizzion's mission is to enable users to securely access applications and data from any device, anywhere increasing mobility and productivity. To learn more about Dizzion, visit **www.dizzion.com**.

Dizzion's PCI DSS compliant virtual desktops are independently audited and verified by QSA Coalfire.

LEARN MORE ⟶