PCI DSS compliance: best practice checklist.

Sycurio.

With a multitude of systems, people, and processes within the call and contact centre, securing sensitive customer data has become increasingly challenging.

Thankfully, we have the Payment Card Industry Data Security Standard (PCI DSS) to help address these ongoing challenges and ensure the protection of customers' most sensitive data.

Less than

30%

of businesses achieve **100%** PCI DSS compliance[1]

However, while the PCI standards can help prevent data breaches that could damage your company's reputation, many businesses still struggle to meet their compliance obligations.

If you are unsure where to begin in evaluating your compliance efforts, follow these simple steps.

Understand how your people and processes deal with payment card information.

Do you know what actually happens when your business handles payment card data? Spend time to understand the technologies in play and the components that are exposed to card data, as well as the data itself. In a contact centre context, card holder (and sensitive authorisation) data includes the Primary Account Number (PAN), security validation codes, and PINs regardless of the form or media type. In addition, digitised voice, voice recordings, recordings of IVR/DTMF tones, images, videos, text data and physical copies all must be protected.

As you observe the ins and outs of how you handle payment data, look for unexpected and "off-the-books" processes. For example, it is not uncommon for contact centre employees to use workarounds and improvisations to complete their jobs, leading to databases full of PANs in the free-form text fields. Similarly, customers may provide card information when it is not needed, and this is then unnecessarily stored.

Figure out where the data flows, where it resides and why it's there.

Negligent employees caused about

62%

of security incidents, costing organisations an average of £240M per incident.[2]

Observe the relationship between your technology and your data.

The PCI DSS requires the protection of card data, not just with the encryption of transmission and data at rest, but also with policies, processes, physical controls, system and network access controls, anti-malware controls, logging and monitoring, patching management, training and awareness. These are controls that must be evaluated across your organisation's entire compliance footprint. As more technologies enter the contact centre, the scope of PCI DSS compliance grows.

For example, Voice-over-IP (VoIP) systems bring networks and connected systems into your PCI DSS scope. They may also support functionality like call cloning/monitoring (which need to be controlled), while the VoIP transmissions themselves must be encrypted.

Likewise, Bluetooth-enabled devices such as headsets and keyboards need to be considered as well. You may also need to protect call recordings with encryption, access controls and logging. If recordings contain Sensitive Authentication Data (SAD), it needs to be removed, or alternately, you must demonstrate that it cannot be mined or queried.

Essential questions to ask when defining the relationship between your technology and data.

As you take a closer look at your technology environment and how it relates to the data you handle, ask the following questions:

- What technology components touch the data and what components support them?
- How large are connected systems' networks?
- What systems that have nothing to do with handling payment data can potentially see the data?
- Are you encrypting all stored and transmitted data?

1. Verizon Payment Security Report 2020. **2.** Ponemon Cost of Insider Threats Report 2022.

PCI DSS compliance: best practice checklist.
(cont)

Sycurio.

- How are you dealing with securely deleting any sensitive authentication data?
- How are you managing the risk associated with technology limitations?
- Are you outsourcing any of this function or any support for this function?
    - How do you know that security and compliance objectives are met?
    - How will you demonstrate these functions' compliance?
- Do you know your compliance status?
- Are there other risk mitigations or controls that need to be accounted for to support your compliance?

Create an action plan.

Once you understand your data, how it's handled and the technologies involved, it is time to create a plan of action. This involves first performing a gap analysis, applying risk analysis to the results and finally, planning your remediation. Some measures will be clear and obvious, while others will be trickier, requiring careful consideration of the intent of PCI DSS and specific risks.

There are many considerations to take into account, but there are several to pay particular attention to when performing a gap analysis.

PCI DSS compliance considerations checklist.

When preparing to make your environment PCI DSS compliant, be sure to consider the following:

- Think about your business processes
    - Remove data you don't need - to reduce risk, and achieve and sustain compliance
    - Support this with training and awareness initiatives
- Consider technological steps to reduce the size of your compliance footprint
- Spend time on the tricky problems to make sure your solutions are justified and defensible based on risk
- Validate your solutions and approaches
- Pay attention to the due diligence and formalisation of specific PCI DSS responsibilities required when outsourcing
- Address any data clean-up issues
- Do not make assumptions or ignore issues

Evaluate new technologies.

If your plan involves evaluating new technologies, take the time to make sure these meet both your needs and PCI DSS requirements. For example, encrypting payment terminals, while useful in card present solutions, only simplify outbound acceptance channels. You still need to address the inbound channels (such as calls, faxes, and letters) and tokenisation – in other words you'll simplify requirements where you need to store card data but leave inbound channels unaddressed.

Also consider the accreditations (like PCI DSS Level 1 Solution Provider) organisations have. Third party accreditations help ensure the legitimacy of the solution.

Finally, consider whether your solutions will hold up over time and against the inevitability of human error. Use risk as your guide, but make sure an actionable plan is in place.

Remember, a security breach of any kind - not just a card data breach - is extremely harmful to your business. By taking the right steps to ensure PCI DSS compliance within your contact centre – the most vulnerable channel – you are demonstrating your commitment to your customers, thereby setting your organisation up for success.

PCI DSS compliance in the contact centre with Sycurio.

To reduce the risk of fraud – and achieve PCI DSS compliance – you need to prevent card holder data flowing through your call recordings, agents, desktops, IT systems, the physical environment and telephony network. And that's where Sycurio's patented data capture solutions can help.

A proven, accredited, and award-winning PCI DSS compliance solution that prevents payment card data from entering the contact centre in the first place, Sycurio.Voice makes it possible for organisations to achieve PCI DSS compliance while recording calls in their entirety.

Customers simply enter their card number directly into the telephone keypad rather than saying them out loud. These numbers are sent straight to the Payment Service Provider (PSP), so sensitive card details never enter the contact centre infrastructure. Additionally, the caller and your agent remain in full voice communication throughout the process, allowing for assistance if the need arises.

And while the call recording captures all voice communications, all DTMF tones are masked so only a flat tone is recorded – making it impossible for agents to recognise numbers or reverse engineer any card data from the call recording itself.