Contact centre security

A guide to PCI DSS compliance in call and contact centres

An insights paper

Contact centre security

A guide to PCI DSS compliance in call and contact centres

Will call centres ever look the same again?

The objective of the Payment Card Industry Data Security Standard (PCI DSS) is to provide a consistent baseline of security controls across all entities that store, process or transmit cardholder data. The standard applies to any organization which interacts with or could impact the security of cardholder data.

In this insights paper, we will focus on PCI DSS compliance from the perspective of contact centres as these will often be at the heart of an organization's customer interaction and payment handling. In our experience, where cardholder data is typically processed in these environments, it can add significant levels of complexity and effort for the organization trying to achieve PCI DSS compliance.

This complexity combined with the current working from home scenario, means that the situation is even further complicated, and the question has to be asked, will call centres ever look the same again?

This paper will consider two scenarios – internal contact centre and the agent working from home scenario. For each scenario the following will be considered:

1. The internal contact centre scenario
2. The agent working from home scenario

Reach out to our PCI DSS expert

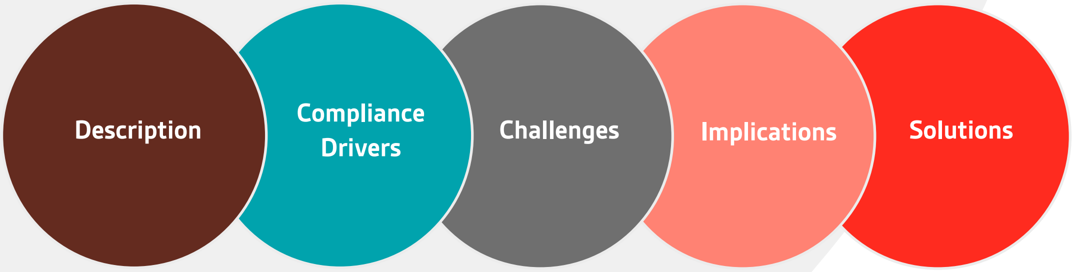
John Hetherton
Global Practice Lead,
PCI DSS

John is an experienced information security, risk, and compliance advisor with more than 10 years' experience in information security. John has been a PCI Certified QSA since 2013 and has conducted many Level 1 PCI DSS audits as well as assisted numerous organizations to de-risk their card holder data environments, in both proactive and post breach scenarios.

Get in touch

Learn more about our PCI DSS consultancy services

Scenario outline



Description

Compliance Drivers

Challenges

Implications

Solutions

Complexity

Handling cardholder data (CHD) over a telephony network has three main challenges from an information security and compliance perspective:

1. Risk of internal fraud from employees handling card data
2. Risk of exponential PCI DSS scope creep where cardholder data is transmitted over the telephony-network
3. Managing legacy call recordings which may include sensitive data stored in clear text

In 2020 and into 2021 the COVID-19 pandemic has caused significant challenges in this space, but also presents an opportunity for contact centres. We will delve into the specific challenges and opportunities later in this document, but let us take a moment to acknowledge what the PCI council has to says on the topic of scoping:

"Accepting spoken or unmasked account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected, in scope for PCI DSS." – Payment Card Industry Security Standards Council (PCI SSC).

There are several use cases where PCI comes into scope for a contact centre environment. In this article we will discuss the typical challenges, thought processes and solutions a business will consider when PCI DSS enters the conversation.

Our approach

BSI work with and validate compliance for many Business Process Outsourcers (BPOs) across the globe, as well as large organizations who utilise internal contact centres for payment processing. These often facilitate bookings, purchasing a service or product, handling chargebacks, or first line support which may involve real time payment handling.

Our consultants have an acute understanding of the complexities of certifying contact centres to a Level 1 PCI DSS compliant standard and importantly how compliance can be achieved in a manner which facilitates frictionless payment processing with high levels of security and compliance. Throughout this paper, you will see insights into different processing scenarios and understand a QSAs perspective to how best to meet compliance obligations. Controls are suggested for consideration where users are working on shared home networks.

These are the types of controls that should be considered in a compensating control scenario and will facilitate beneficial dialogue with your QSA and acquiring bank, should they query the controls surrounding the people, processes and technologies currently used to process cardholder data.

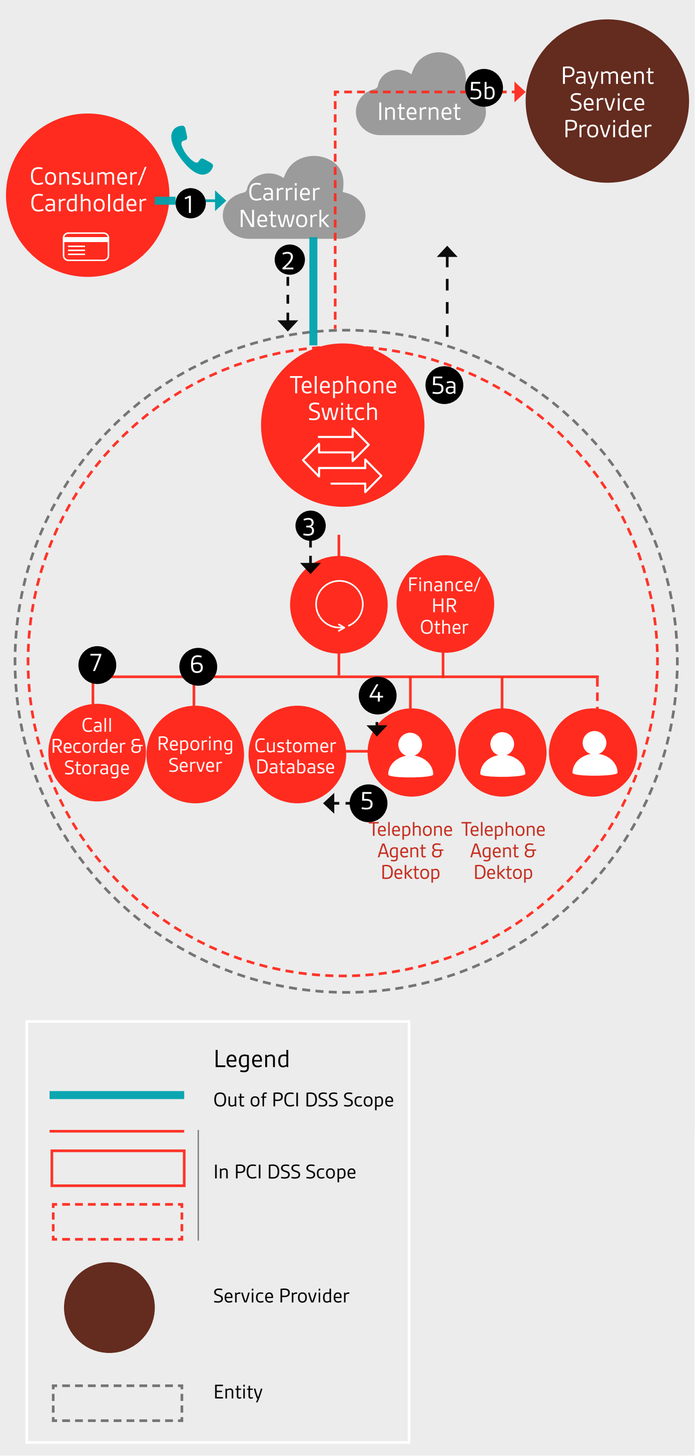
"Accepting spoken or unmasked account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected, in scope for PCI DSS."

Payment Card Industry Security Standards Council (PCI SSC)

Scenario 1
Internal contact centre

The following use case and diagram depicts a typical call centre scenario that could be applied to paying a bill or purchasing goods or services.

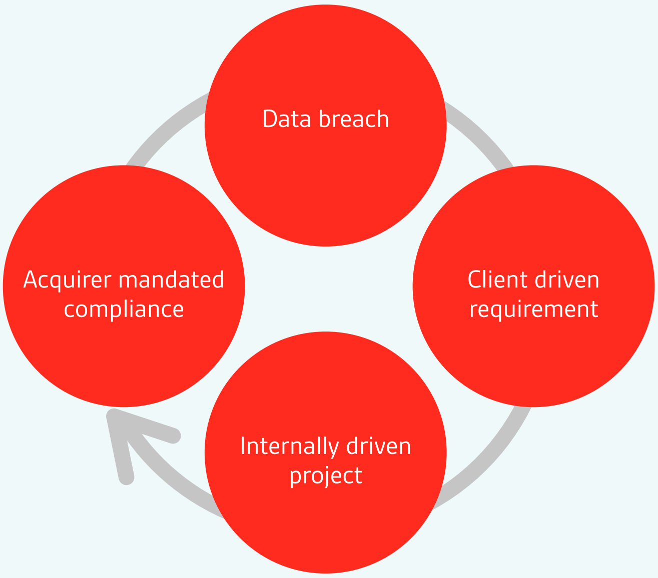
Use Case Description



Source: PCI Security Standards – Protecting Telephone Based Payment Card Data

Step 1	The customer is connected to the agent and call recording has started, as part of the dialogue when asked they provide their account data to the agent.
Step 2	The spoken account data enters the telephone environment via the telephone switch.
Step 3	The account data is transmitted by the entities voice and network to the agent.
Step 4	The agent inputs the account data into their desktop PC via the keyboard.
Step 5	Customer data is entered into the customer relationship management system (CRM) where it is processed (assume no CHD stored).
Step 5a	The account data is transmitted to the Payment Service Provider (PSP) or acquirer. For example, this may occur via data input into an application on the agent's desktop, via a virtual terminal accessed hosted by the PSP or acquirer over a secure internet connection from the agent's desktop, or via a physical point of interaction (POI) payment terminal.
Step 5b	The PSP processes and potentially stores Card Holder Data (CHD) and returns a payment validation reference to the agent desktop or payment terminal.
Step 6	The interaction is recorded on the reporting server.
Step 7	The call-recording equipment attached to the network captures the account data, and the account data is stored in call recording storage. Call recording ceases. It is indexed and stored. As this point, call data can be queried.

Compliance drivers


Data breach
Client driven requirement
Internally driven project
Acquirer mandated compliance

Challenges

Based on the way this network is set up, the PCI DSS scope is extensive, and when the organization operates a flat network structure, it would include all people, processes and technology on that connected flat network.

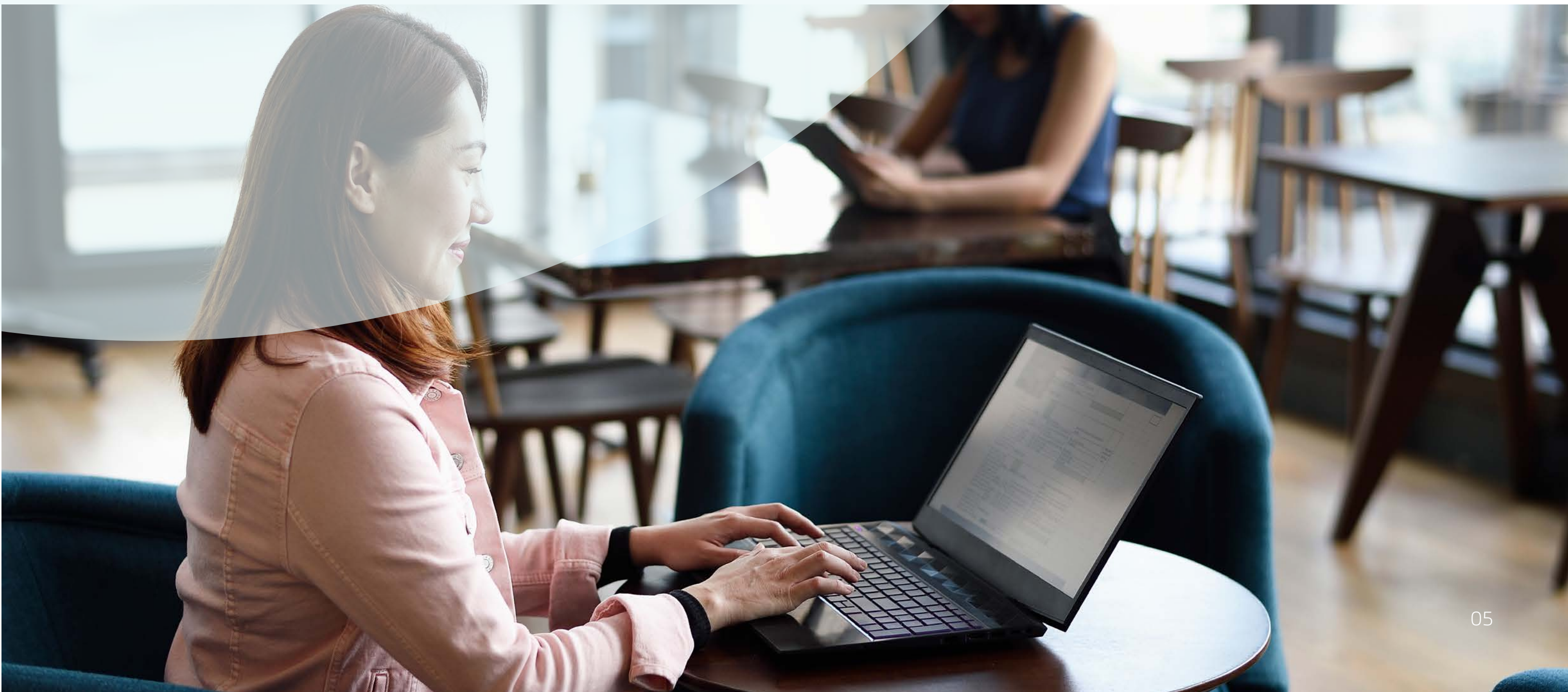
Implications

Having the entire network in scope for PCI DSS compliance can introduce a significant overhead in terms of people, time, and financial resources required to implement and maintain compliance on an ongoing basis. Depending on volume of transactions, either Self-Assessment Questionnaire D (SAQ D) or a Report on Compliance (ROC) would be applicable to the entire environment.

Solutions

Where the organization must continue to offer a telephony-based payment channel the following options to reduce scope exist:

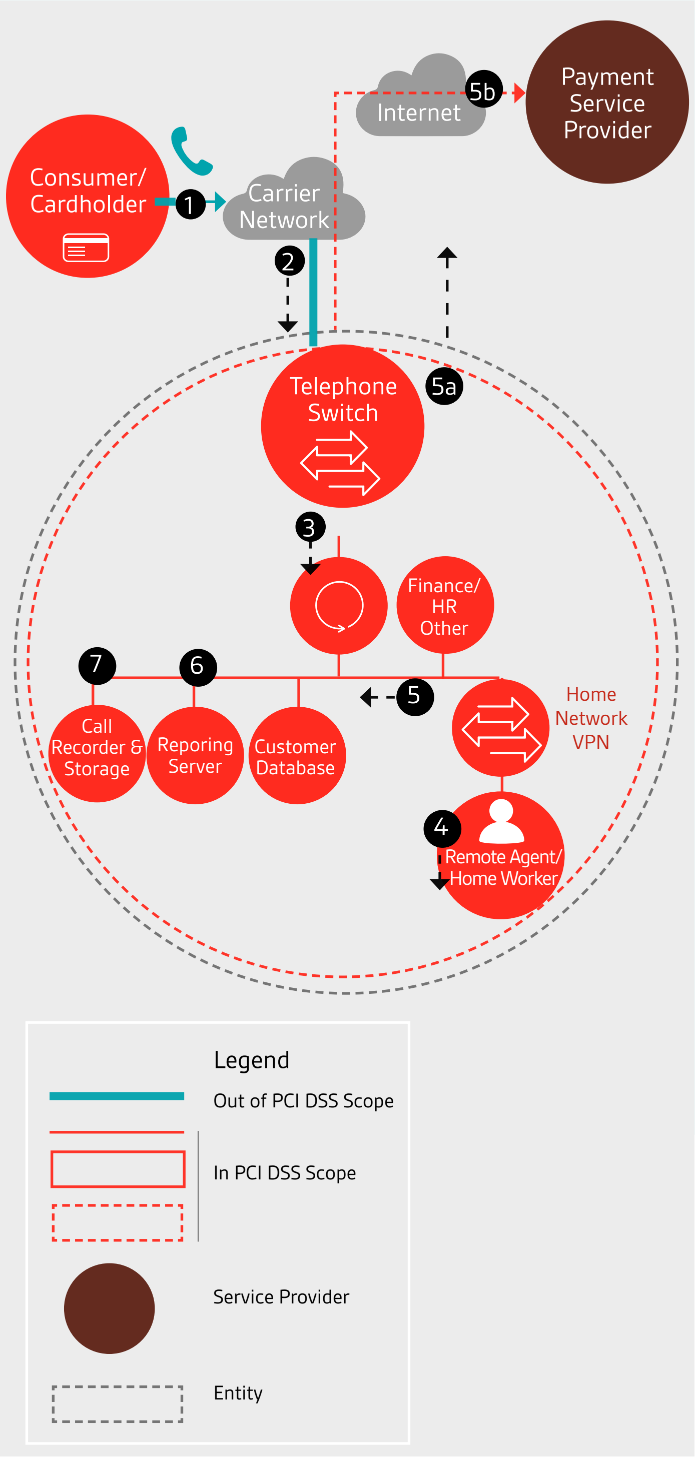
	Scope reduction options	Typical attestation
1.a	Leverage a cloud-based PCI DSS compliant Dual Tone Multi Frequency (DTMF) masking solution to proxy and remove card data from the call centre environment. Legacy call recordings will need to be deleted from the environment or masked / redacted.	SAQ – A
1.b	Where DTMF is not an option, (often with BPOs) considerations should be given to reduce the number of systems in scope by segmenting systems connected to those which directly store process or transmit cardholder data. Systems will still be in scope for SAQ D, but applicable to a smaller footprint, reducing the overall compliance effort. An internally managed, dedicated and segmented internal IVR solution may also provide an option for a reduced scope. Legacy call recordings will need to be deleted from the environment or masked / redacted.	SAQ – D
1.c	Use a system which allows call centre agents to generate one-time payment links to be sent to a customer's smart phone. This is suitable typically for small business, low volume transactions. Legacy call recordings will need to be deleted from the environment or masked / redacted.	SAQ - A



Scenario 2
Agents working from home and processing cardholder data

A call centre agent working from home, using a corporate managed end point and softphone, over VPN, to process cardholder data.

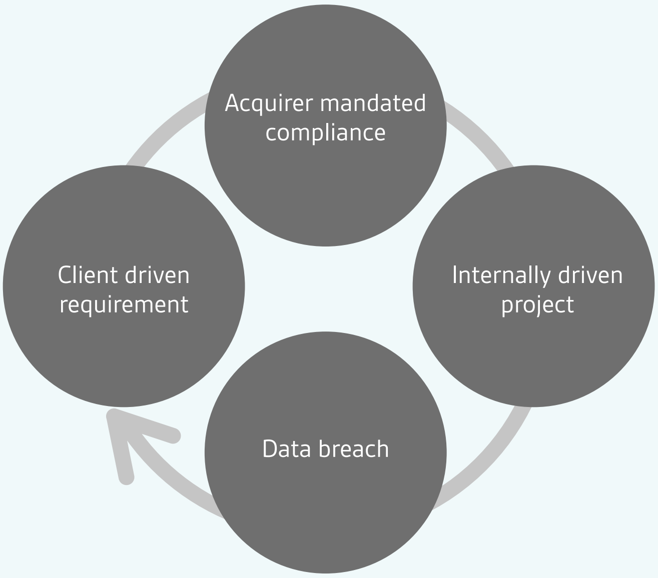
Use Case Description



Step 1	The customer is connected to the agent and call recording has started, as part of the dialogue when asked they provide their account data to the agent.
Step 2	The spoken account data enters the telephone environment via the telephone switch.
Step 3	The account data is transmitted by the entities voice and network to the agent via a softphone application on the corporate managed end point. The agent's end point is connected to their local WiFi Router and Network.
Step 4	The agent inputs the account data into their end point via the keyboard, which is transmitted over the VPN to the corporate network.
Step 5	Customer data is entered into the customer relationship management system (CRM) where it is processed, not stored.
Step 5a	The account data is transmitted to the Payment Service Provider (PSP) or acquirer. For example, this may occur via data input into an application on the agents desktop, via a virtual terminal hosted by the PSP or acquirer over a secure internet connection from the agent's desktop.
Step 5b	The PSP processes and potentially stores Card Holder Data (CHD) and returns a payment validation reference to the agent desktop or payment terminal.
Step 6	The interaction is recorded on the reporting server.
Step 7	The call-recording equipment attached to the network captures the account data, and the account data is stored in call recording storage. Call recording ceases. It is indexed and stored. As this point, call data can be queried.

Source: PCI Security Standards – Protecting Telephone Based Payment Card Data

Compliance drivers


Acquirer mandated compliance
Internally driven project
Data breach
Client driven requirement

The following should be considered in addition to the previously mentioned items in Scenario 1.

Challenges

We have a further complicated scenario when staff are working from home and connecting through their local network as the end point is part of the CDE (directly processing account data) thus systems connected to the end point are also in scope. That means the users home network and devices on the same LAN are in scope.

Implications

It becomes very difficult (almost impossible) to accurately scope the environment, and further to make non-corporate managed devices PCI DSS compliant.

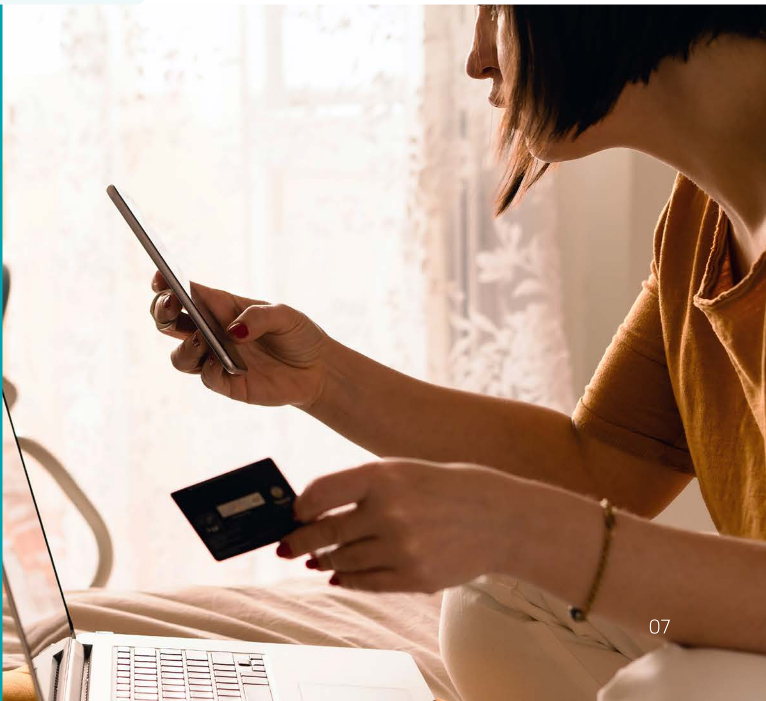
Solutions

Where the organization must continue to offer a telephony-based payment channel the following options to reduce scope exist:

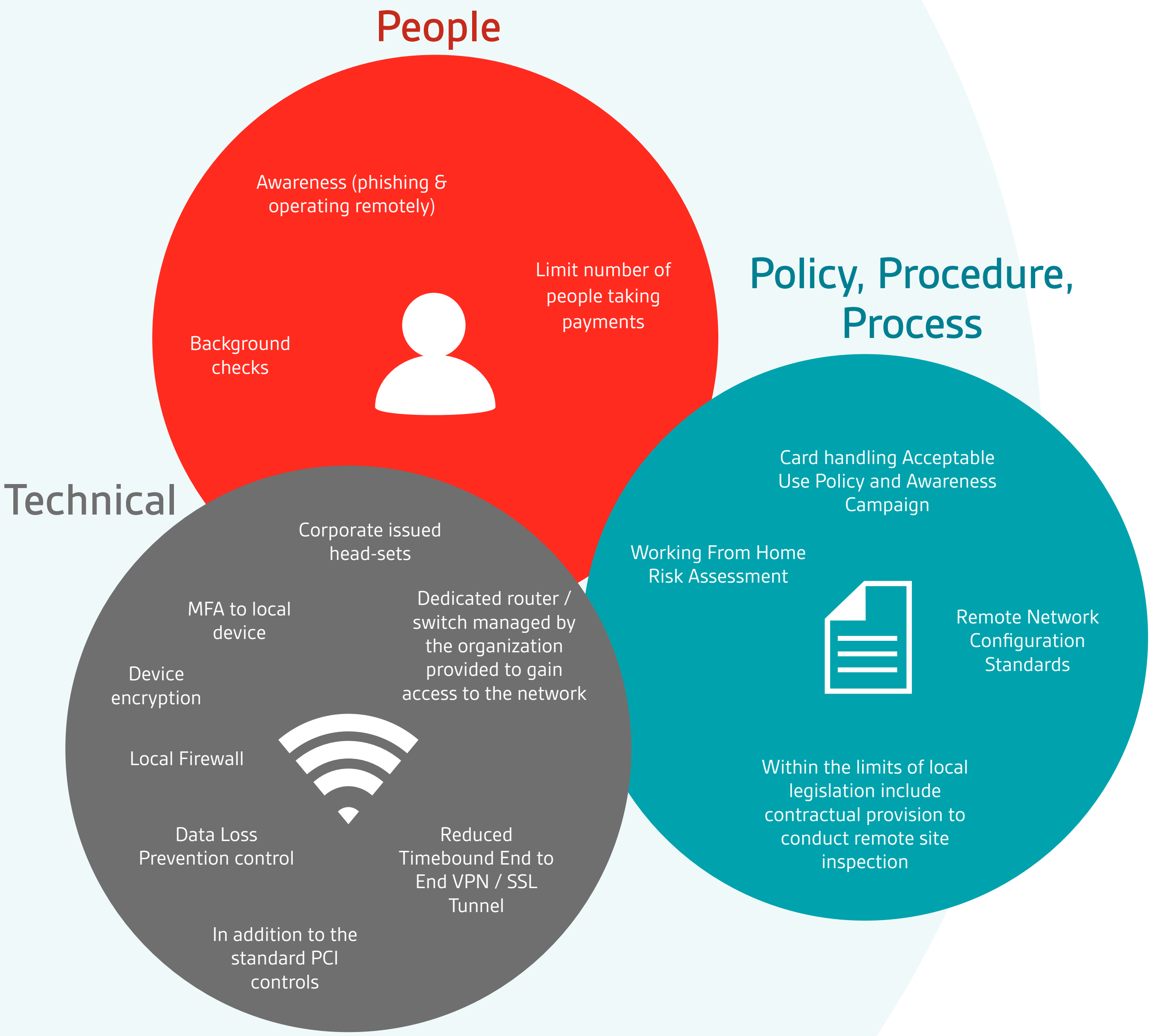
	Scope reduction options	Typical
1.a	Leverage a cloud-based PCI DSS compliant DTMF masking solution to proxy and remove card data from the call centre environment. This can descope the environment, but legacy call recording which include clear text account data will need to be removed if they exist.	SAQ – A
1.b	Where DTMF is not an option, (Often with BPOs) considerations should be given to reduce the number of systems in scope by segmenting systems connected to those which directly store process or transmit cardholder data. The path of least resistance in this scenario is to provide the user with a dedicated service / device to access the internet, removing their home network from scope. As well as all the existing PCI DSS requirements applicable, this would include providing agents with a pre-configured, secure and compliant router/firewall / or dedicated SIM enabled internet connection managed by the entity which will only allow connectivity via the corporate managed VPN, thus removing their local network from scope. Implementing a policy and awareness plan to strongly underscore the organizations "Acceptable card data handling" requirements, which will cover many areas including prohibiting writing down, recording or other storage of account data, working in a secure area, secure storage of organizational equipment. Conducting an internal risk assessment to cover threats, vulnerabilities, likelihood and impacts associated with an increased level of exposure to card data theft / Fraud due to staff now working from home. Some additional risk mitigations that should be considered in the assessment are included in the Controls Section overleaf.	SAQ – D

> "Once the risk is appropriately managed and compliance can be demonstrated to PCI DSS, there is no reason that contact centre staff working from home, should introduce a barrier to compliance going forward, giving greater flexibility to organization in the deployment of resources."

John Hetherton, Global Practice Lead - PCI DSS, BSI



Controls



People

Awareness (phishing & operating remotely)

Limit number of people taking payments

Background checks

Policy, Procedure, Process

Card handling Acceptable Use Policy and Awareness Campaign

Working From Home Risk Assessment

Remote Network Configuration Standards

Within the limits of local legislation include contractual provision to conduct remote site inspection

Technical

Corporate issued head-sets

MFA to local device

Dedicated router / switch managed by the organization provided to gain access to the network

Device encryption

Local Firewall

Data Loss Prevention control

Reduced Timebound End to End VPN / SSL Tunnel

In addition to the standard PCI controls

How can BSI help?

BSI is a certified Qualified Security Assessor (QSA). In addition to providing senior resources to validate and attest compliance to PCI DSS, BSI can provide support in the development of appropriate risk assessments, mitigations, secure solution designs and awareness content to ensure that the end-to-end approach adopts a defensible and robust approach to maintaining PCI DSS compliance in a work from home scenario.

About PCI

Organizations that store, process or transmit payment card information are mandated by VISA, MasterCard and the other major participating card brands to meet the security requirements included in the Payment Card Industry Data Security Standard (PCI DSS).

Compliance requirements are typically drive from acquiring banks for Merchants, and by Clients for Services Providers.

The level at which and types of attestations which merchants and service providers must attest are driven by the number of card numbers they see per annuum and way they process the data.

With our team of security experts and certified PCI QSAs, BSI helps ensuring that PCI compliance requirements are implemented into your organization effectively. We provide consultancy services from the very early stage of the compliance roadmap (for instance defining the scope of the requirements) to validating them with a formal PCI Assessment, penetration testing and issuing the Attestation of Compliance.

Our PCI DSS consultancy services:

- Solution Design Workshop
- PCI DSS scope determination and scope reduction services
- PCI DSS gap analysis and prioritized action planning
- PCI DSS Implementation Support and PCI Self-Assessment Questionnaire (SAQ)
- PCI DSS Report on Compliance (ROC) audit
- P2PE implementation assessments
- Penetration testing and vulnerability scanning services
- ASV Scanning

Get in touch

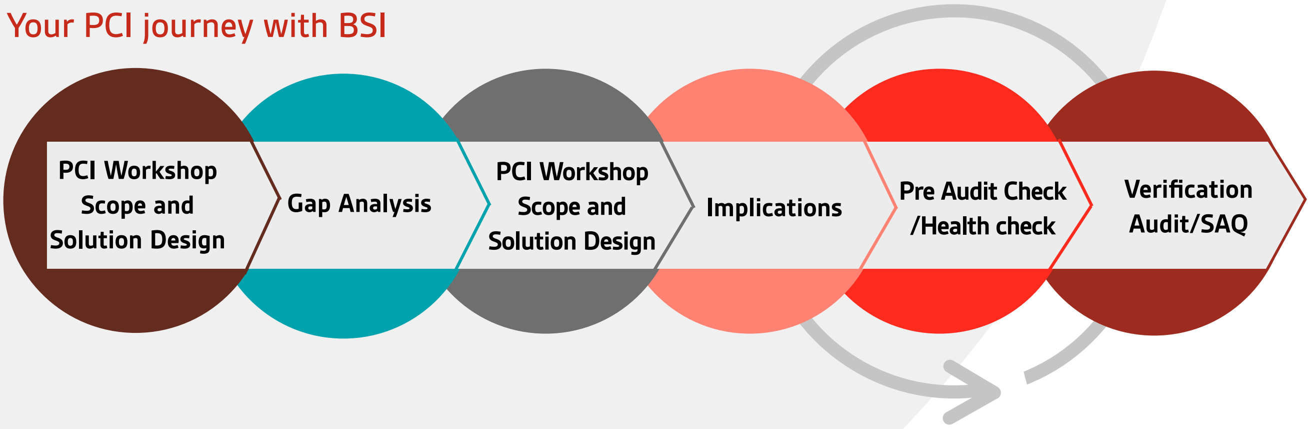
Speak to us about how we can help you support your PCI DSS requirements.

✉ Contact us directly

🌐 Learn more about our PCI DSS consultancy services

Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.

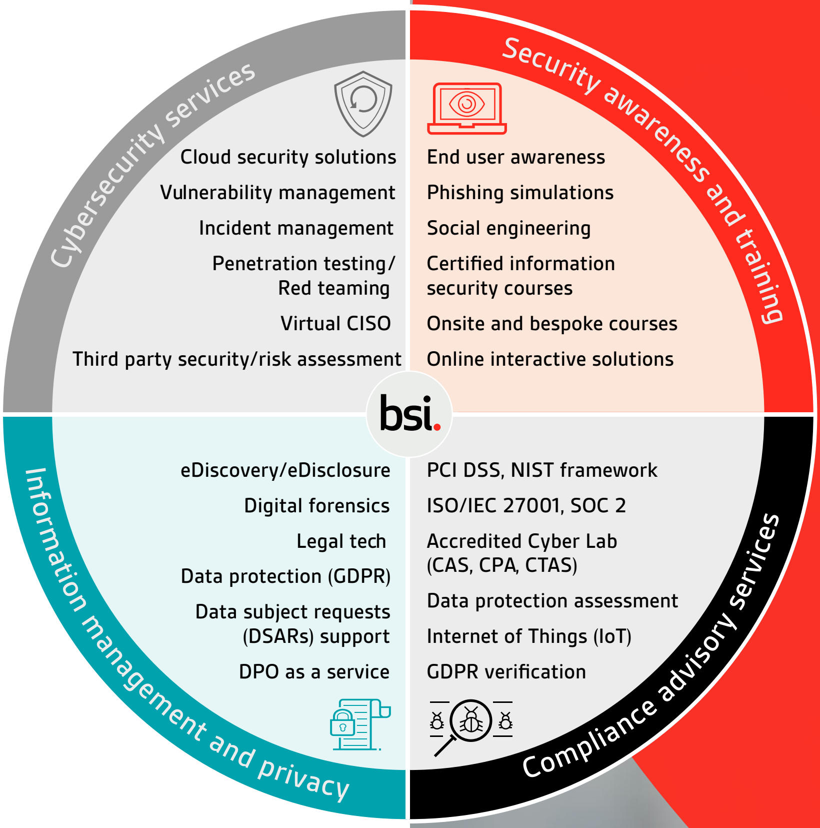
Your PCI journey with BSI


PCI Workshop Scope and Solution Design
Gap Analysis
PCI Workshop Scope and Solution Design
Implications
Pre Audit Check /Health check
Verification Audit/SAQ

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Services include:



Cybersecurity services

Cloud security solutions
Vulnerability management
Incident management
Penetration testing/ Red teaming
Virtual CISO
Third party security/risk assessment

Security awareness and training

End user awareness
Phishing simulations
Social engineering
Certified information security courses
Onsite and bespoke courses
Online interactive solutions

Information management and privacy

eDiscovery/eDisclosure
Digital forensics
Legal tech
Data protection (GDPR)
Data subject requests (DSARs) support
DPO as a service

Compliance advisory services

PCI DSS, NIST framework
ISO/IEC 27001, SOC 2
Accredited Cyber Lab (CAS, CPA, CTAS)
Data protection assessment
Internet of Things (IoT)
GDPR verification

Our expertise is accredited by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

Find out more

EMEA	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: cyber.ie@bsigroup.com	cyber@bsigroup.com	cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-ie	bsigroup.com/cyber-uk	bsigroup.com/cyber-us

bsi.

Subscribe to our newsletter

Follow us on