PCI DSS Reference Guide.

Navigating the Payment Card Industry Data Security Standard (PCI DSS)

We are Eckoh.

Leading organizations **trust** Eckoh's data payment security solutions.

Since 2009, Eckoh has **transformed** contact centers across a range of sectors to be **efficient**, **secure** and **PCI DSS compliant**.

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

With a long 20-year legacy of creating award-winning, efficient customer engagement automation solutions for contact centers, Eckoh is also a master in designing the most future-facing, flexible and robust payment security solutions for this market. Adjusting to changes in regulations, operating models, and customer behavior, we can make rapid and agile modifications to business processes without disruption to existing systems.

We constantly audit, research and innovate so that you can stay ahead of the competition, applying the latest techniques in first-class security technology within our customer engagement tools.

What’s in store?

1\.
Protecting cardholder data in contact centers

2\.
Who does PCI compliance apply to?

Merchants

Service Providers

3\.
PCI compliance requirements

4\.
The cost of non-compliance

5\.
Become PCI compliant

Click on the icons below to jump to the page.

1. Protecting cardholder data.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards mandated by the world's major card brands. Today, any organization that processes, stores, or transmits cardholder data must abide by the standard.

PCI DSS is always evolving – reflecting shifts in technology, emerging threats from fraud, theft, and data breaches. Security standards are rising and the costs of failures are increasing. It's **critical to note** that the personal data covered by PCI DSS also falls within the scope of the General Data Protection Regulation (GDPR) and a raft of other privacy legislation in the US and globally.

In 2018, The PCI Security Standards Council **(PCI SSC)** released supplemental information about securing payments in a card-not-present environment such as contact centers.

This guidance is based on the three pillars of people, process, and technology and the unique risks in sensitive cardholder data being transmitted in card-not-present transactions. For example, a customer providing their credit card number, expiration date, and security code with a live agent in a contact center exposes cardholder data to the customer's phone carrier network, call recordings, servers, agent desktops, the agent, and so much more.

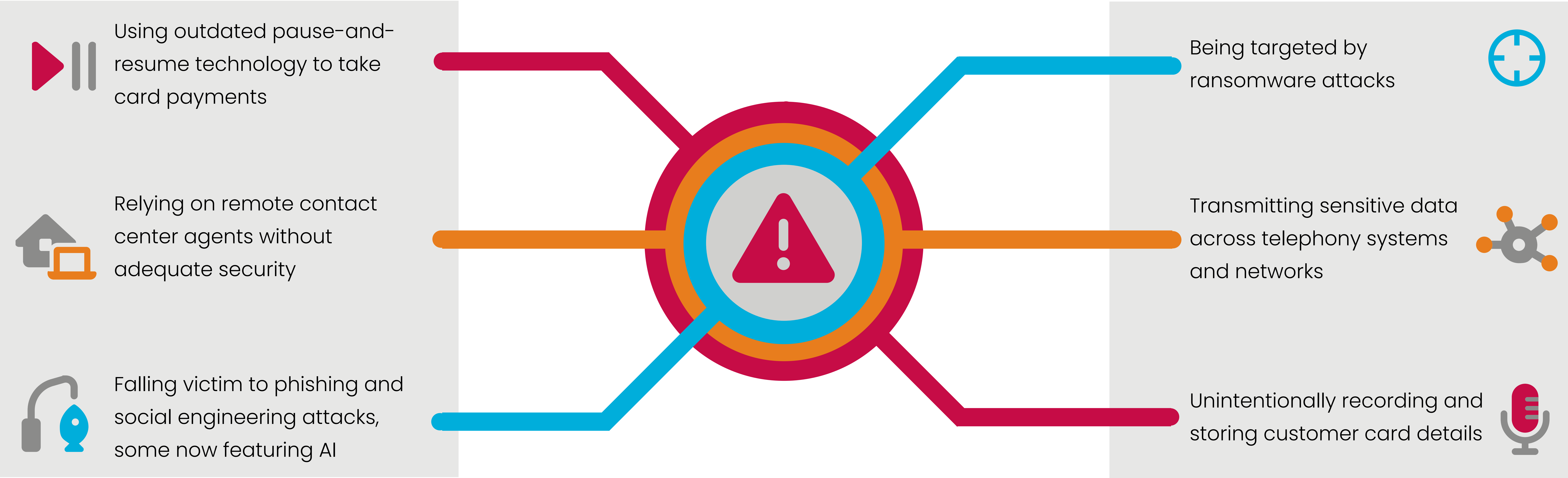
Because of this increased attack surface and more companies moving to cloud solutions, the PCI SSC deems it critical to make telephone-based payments, especially those made over Voice over Internet Protocol **(VoIP),** in-scope for PCI DSS requirements.

The world continues to change at speed – with new contact platforms, payment methods, and more contact center agents working remotely. The standard was strengthened considerably with the arrival of PCI DSS 4.0, with 13 changes required by March 2025 and another 51 for March 2025. Put simply, compliance has become more complex and demanding.

1. Protecting cardholder data.

The attack surface continues to evolve. As business and technologies change, criminals have become more opportunistic, adept, and sophisticated in how they attempt to steal valuable consumer data, including cardholder details.

Contact centers may be especially at risk in these areas:



Using outdated pause-and-resume technology to take card payments

Relying on remote contact center agents without adequate security

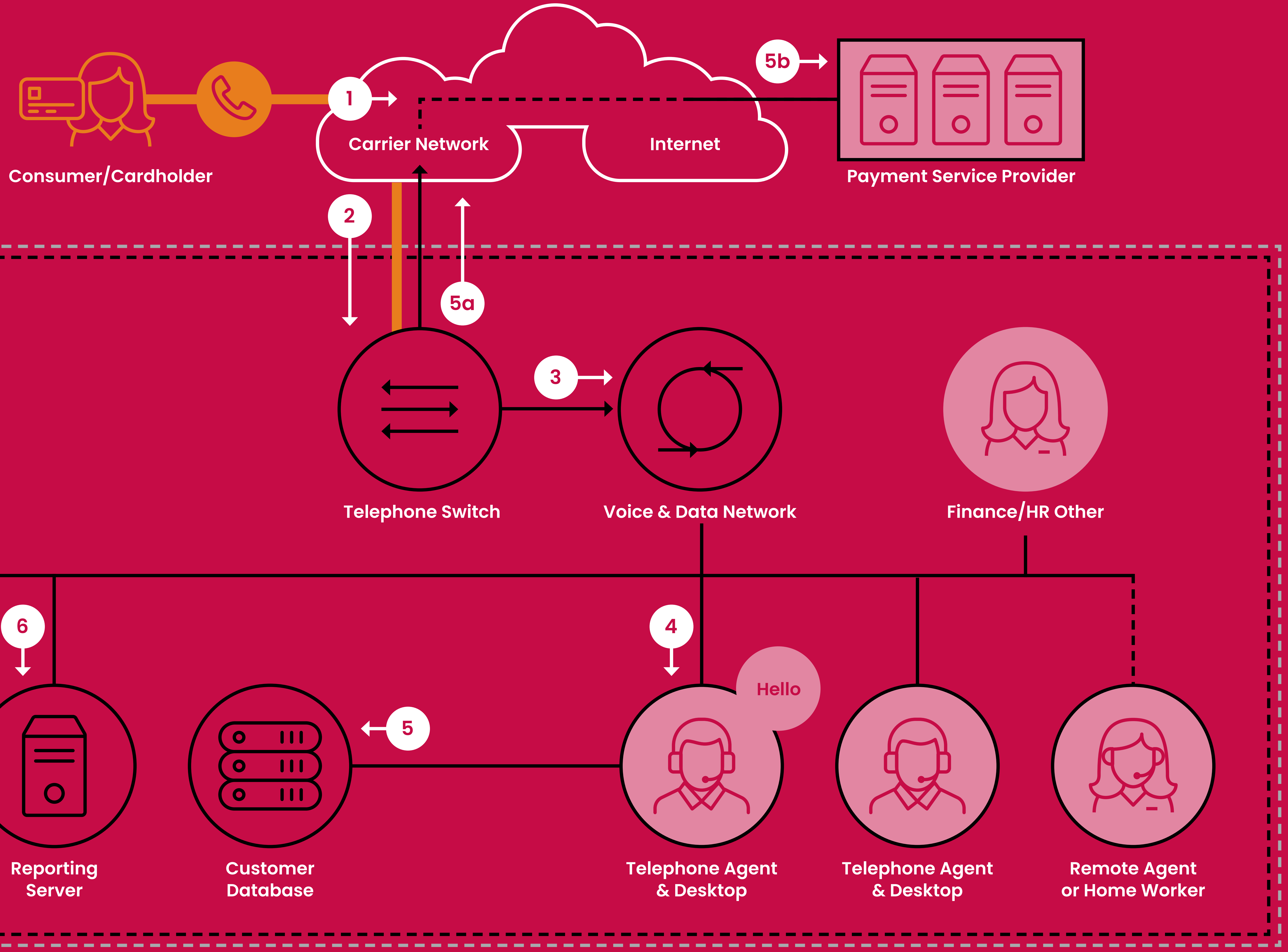
Falling victim to phishing and social engineering attacks, some now featuring AI

Being targeted by ransomware attacks

Transmitting sensitive data across telephony systems and networks

Unintentionally recording and storing customer card details

Call flow.



Legend

- 🟧 Out of PCI DSS Scope
- □ In PCI DSS Scope
- ▨ Service Provider
- ⬚ Entity

2. Who does compliance apply to?

There are two very distinct categories for PCI DSS compliance:

Merchants

Find out more

Service Providers

Find out more

2. Merchants.

As far as the PCI Data Security Standard is concerned, a merchant is any organization that processes, submits, or stores payment data related to the major card brands.

Category	Criteria	Requirement
Level 1	Processes more than six million card transactions on an annual basis or has suffered a hack or an attack that resulted in an Account Data Compromise Event.	Annual PCI DSS assessment resulting in the completion of a Report of Compliance **(ROC).** Quarterly Network scan by an Approved Scanning Vendor (ASV)*
Level 2	Processes one to six million card transactions on an annual basis.	As above.
Level 3	Processes 20,000 to one million card transactions on an annual basis.	As above.
Level 4	All other merchants.	As above

*If the merchant handles online payments

Each card company does have minor differences in their definition for levels in regards to transaction numbers. Some payment providers, partners and clients may require you to level up in order to meet their specific security needs.

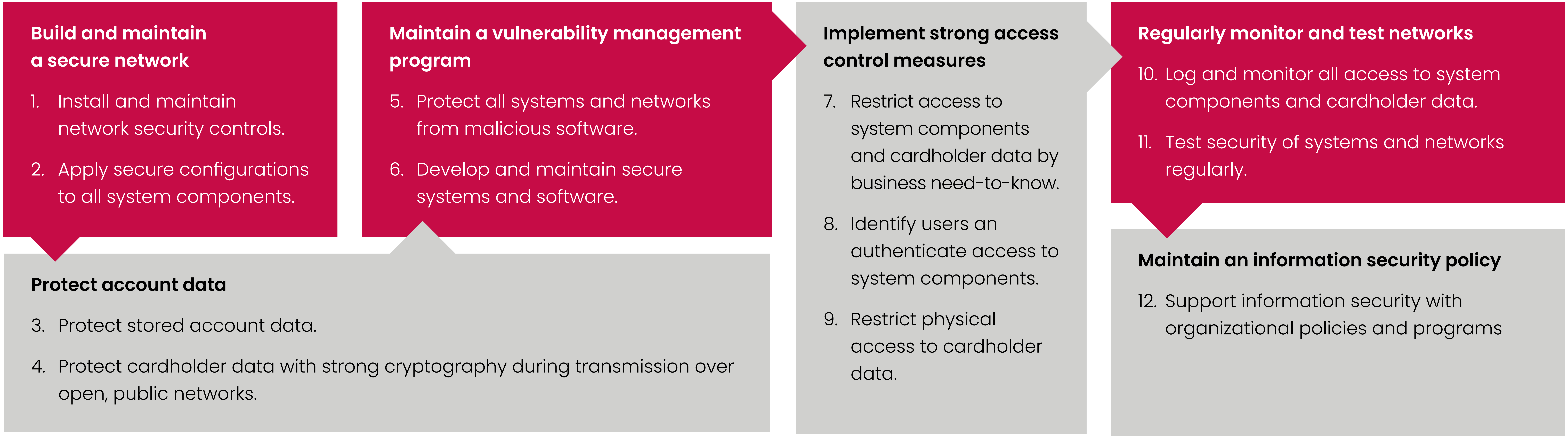
2. Service Providers.

Service providers are defined by the PCI Security Standards Council as any business entity that is not a payment brand that is directly involved with the storing, transmission or processing of payment card data.

Category	Criteria	Requirement
Level 1	Store, transmit or process more than 300,000 card transactions on an annual basis.	• Annual ROC by a Qualified Security Assessor **(QSA)**. • Quarterly Network scan by an Approved Scanning Vendor **(ASV)** • Penetration Test • Internal Scan • Attestation of Compliance Form **(AOC)**
Level 2	Store, transmit or process less than 300,000 card transactions on an annual basis.	• Annual Self-Assessment Questionnaire D **(SAQ-D)** • Quarterly network scan by **ASV** • Penetration Test • Internal Scan • **AOC** Form

3. Compliance requirements.

Within the 12 requirements of PCI DSS, there are hundreds of sub-requirements that go deep into an organization's systems, processes, and environment. Some requirements can be extremely difficult to meet, and so partnering with experts can help.



Build and maintain a secure network

1. Install and maintain network security controls.
2. Apply secure configurations to all system components.

Protect account data

3. Protect stored account data.
4. Protect cardholder data with strong cryptography during transmission over open, public networks.

Maintain a vulnerability management program

5. Protect all systems and networks from malicious software.
6. Develop and maintain secure systems and software.

Implement strong access control measures

7. Restrict access to system components and cardholder data by business need-to-know.
8. Identify users an authenticate access to system components.
9. Restrict physical access to cardholder data.

Regularly monitor and test networks

10. Log and monitor all access to system components and cardholder data.
11. Test security of systems and networks regularly.

Maintain an information security policy

12. Support information security with organizational policies and programs

4. Cost of non-compliance.

Security failures can be devastating for organizations. Data breaches can expose non-compliance with PCI DSS. The impact can be felt across the business in multiple ways – and costs begin to snowball.

Cost of investigation

Organizations must spend time and money understanding what's happened – and which data has been compromised.

Remediation measures

Systems and data must be protected quickly, while customers need to be kept informed and new card details issued.

Penalties from the card brands

Organizations may be fined by the card brands and pay increased fees on every subsequent card transaction they handle.

Privacy law costs

A data breach may also contravene GDPR and other privacy rules, leading to huge fines.

Reputational damage

As news gets out, confidence in an organization can falter - damaging its share price and the credibility of its leadership.

Cost of a Data Breach.

The precise cost of a data breach will vary between organizations. But IBM's Cost of a Data Breach Report 2024 provides a helpful guide.

Equifax experienced a data breach that exposed the personal information of 147 million people.

The credit agency agreed to pay $575 million — potentially rising to $700 million — in a settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and all 50 U.S. states and territories.

Source: CSO Online

The average total cost of a data breach for a US company is $4.88 million.

Costs have risen sharply. This is up 10% on 2023.

46% of breaches involve customer personal data.

Personal identifiable information (PII) can include cardholder details – a sweet-spot targeted by criminals.

The average total cost of a malicious insider attack for a US company is $4.99 million.

The actions of a rogue employee, for example, can lead to even worse consequences for organizations.

It takes an average of 292 days to identify and contain a breach involving stolen credentials.

292

Responding to a breach is a time-consuming process, taking up valuable operational resources.

Numbers are from IBM analysis of research data compiled by the Ponemon Institute.

5. Become PCI compliant quickly.

Assess

Identify which level of compliance your organization qualifies for.

Analyze your current IT systems and business processes that involve payment data storing, transmitting or processing.

Identify any risks such as pause-and-resume, remote workers or cardholder data being transmitted across your telephone or network.

Remediate

Eliminate the vulnerabilities by partnering with vendors that remove the risk of storing, transmitting or processing cardholder data. The best approach is to never let this sensitive data touch or traverse across any part of your environment or come in contact with any agents.

Put processes in place that reduce your risk level and prepare your organization for responding to a data breach.

Continue

PCI DSS compliance is a continuous process and should be seen as a business-as-usual activity within your organization.

Any vendors you partner with should be innovating – preparing you for new contact channels, payment methods, emerging security threats, and future changes to PCI DSS and privacy laws.

Report

Complete the necessary reporting for your merchant level.

Glossary of terms.

Key terminology

PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
SAQ	Self-Assessment Questionnaire
VoIP	Voice over Internet Protocol
ROC	Report of Compliance
QSA	Qualified Security Assessor
ASV	Approved Scanning Vendor
AOC	Attestation of Compliance

Listed here are the SAQ levels appropriate for contact center environments taking card-not-present payments:

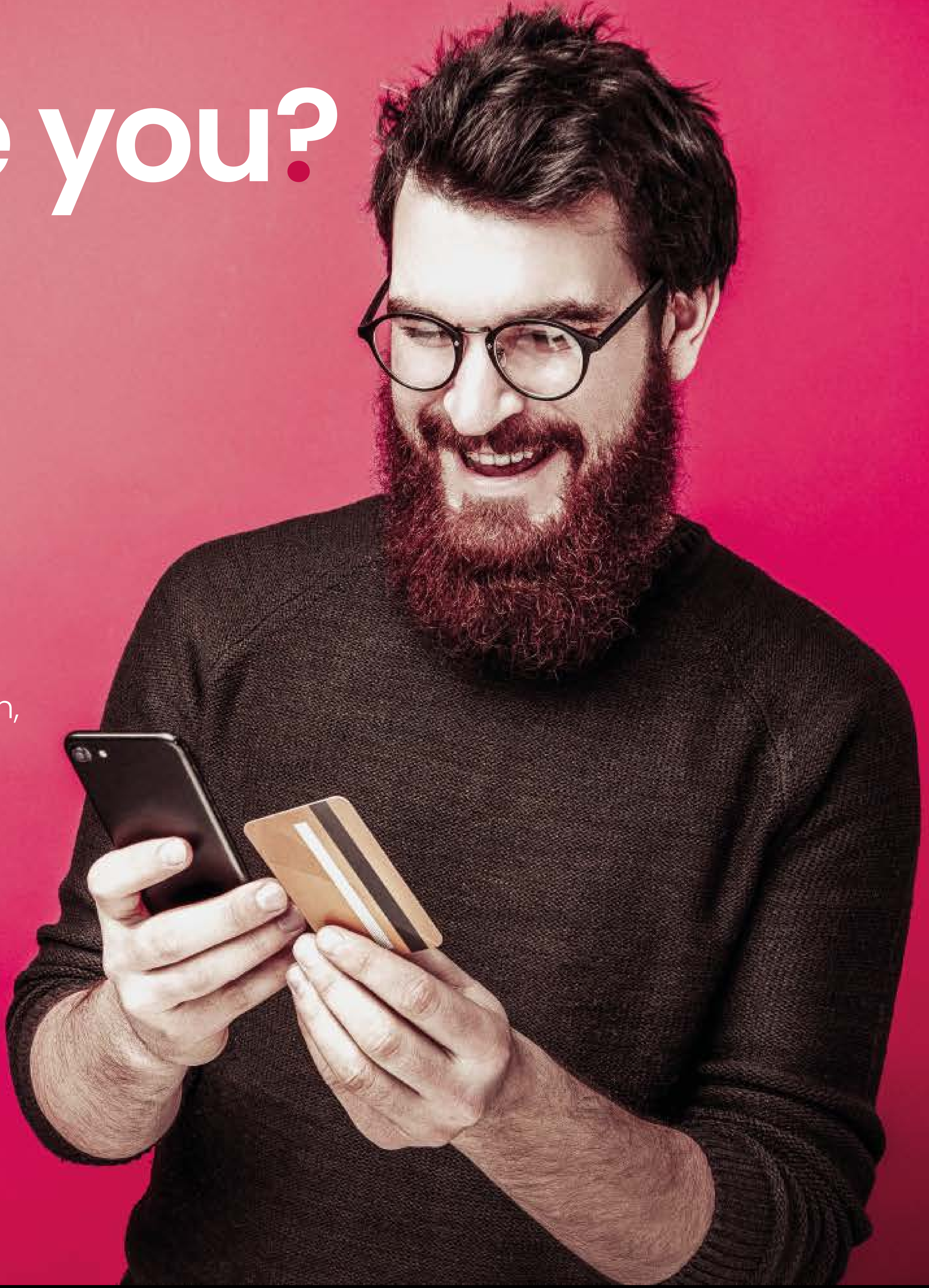
SAQ-A : Using a partner to do the heavy lifting – handling the vast majority of PCI DSS requirements on your behalf

Merchants accepting card-not-present payments, such as over the phone or via ecommerce, that have fully outsourced all PCI DSS functions for storing, transmitting or processing cardholder data. If the merchant is qualified for SAQ-A, no electronic storage, transmission or processing can touch their systems or premises.

SAQ-D : Managing PCI DSS yourself, with all the complexities and expertise required

If the merchant does not meet SAQ-A requirements, they are required to complete an Attestation of Compliance. SAQ-D is the most comprehensive questionnaire and includes provisions for all of the PCI DSS requirements.

We’re ready. Are you?



This Guide to Safe Payments is to inform and educate merchants and other entities involved in payment card processing.

For more information about the **PCI SSC** and the standards we manage, please visit **www.pcisecuritystandards.org**.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Standards or their supporting documents.

Get in touch

www.eckoh.com

Eckoh