

# Payment security masterclass



Payments data security standards  
within the contact centre supply chain

18 January 2022 | 12:30 - 13:15



**Candice Pressinger**  
Director Customer Data  
Elavon



**Jeremy King**  
VP - Regional Head for Europe,  
PCI Security Standards Council



**John Greenwood**  
Director, Compliance3 and  
Head of Technology & Payments,  
Contact Centre Panel



**Simon Turner**  
PCI DSS Advisory Cloud Services  
& Contact Centres (QSA),  
BT Plc

# Purpose and objective

Our purpose today is put the Payment Card Industry Data Security Standard (PCI DSS) into context for those entities that support customer contact centres that take voice and non-voice payments from customers.

These entities include UCaaS and CCaaS vendors, other contact centre application vendors, all resellers of those technologies, as well as the outsourced contact centre community.

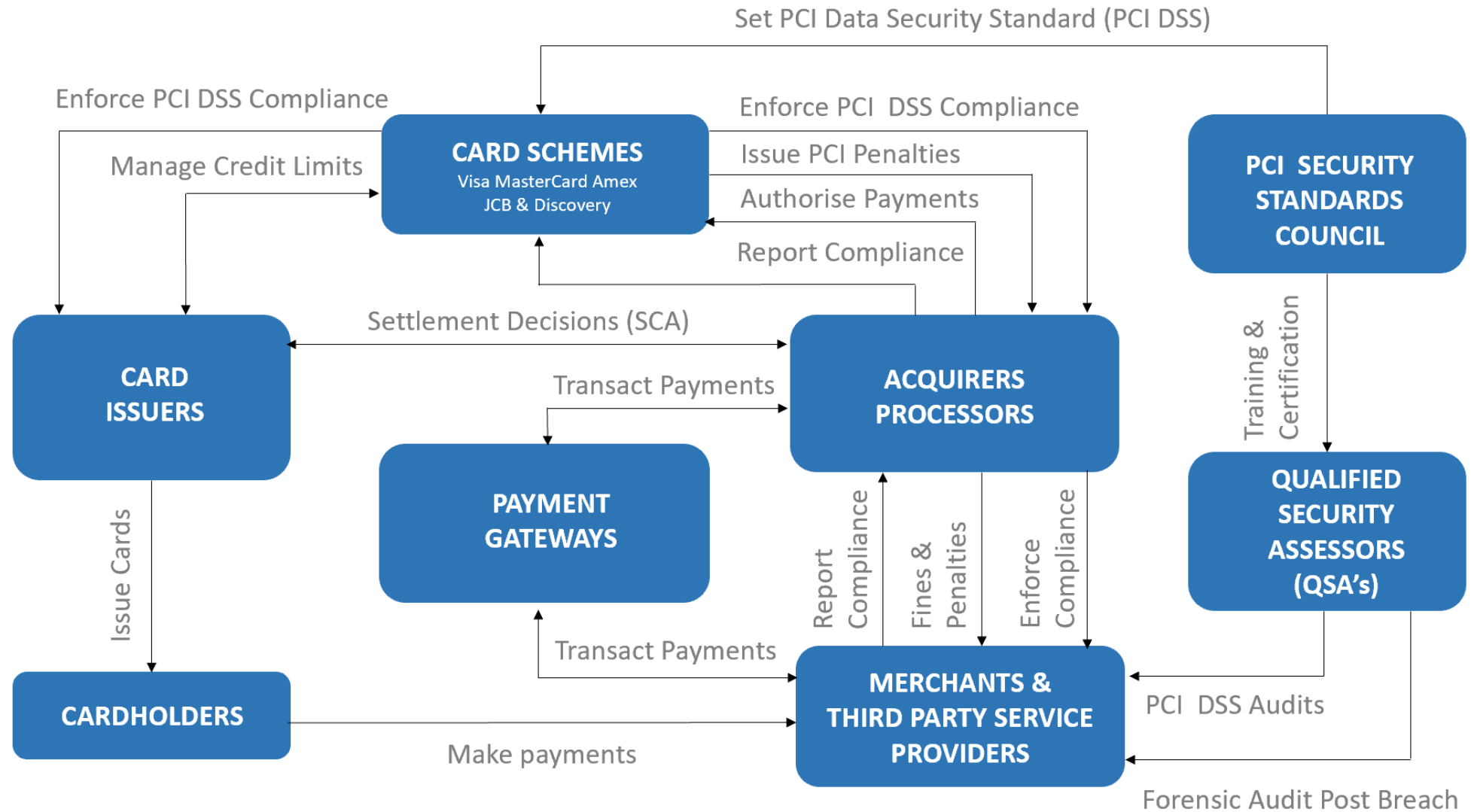
The slides or exhibits in this document will be referenced by our panel during conversation so that we can avoid a slide show, but at the same time provide content that will help your understanding of the question being asked and / or, the topic being discussed.

Our objective is to ensure that your organisation is given the best possible support during and after this session, enabling you to better support your customers own obligations to comply with the PCI DSS.

Please ask questions using the chat function during the session, or if not viewing live, please feel free to reach out directly after the event.

We hope you enjoy the conversation.

# 1. Secure payments ecosystem



## 2. PCI Security Standards Council

<https://www.pcisecuritystandards.org>



**We Help  
Secure  
Payment  
Data**

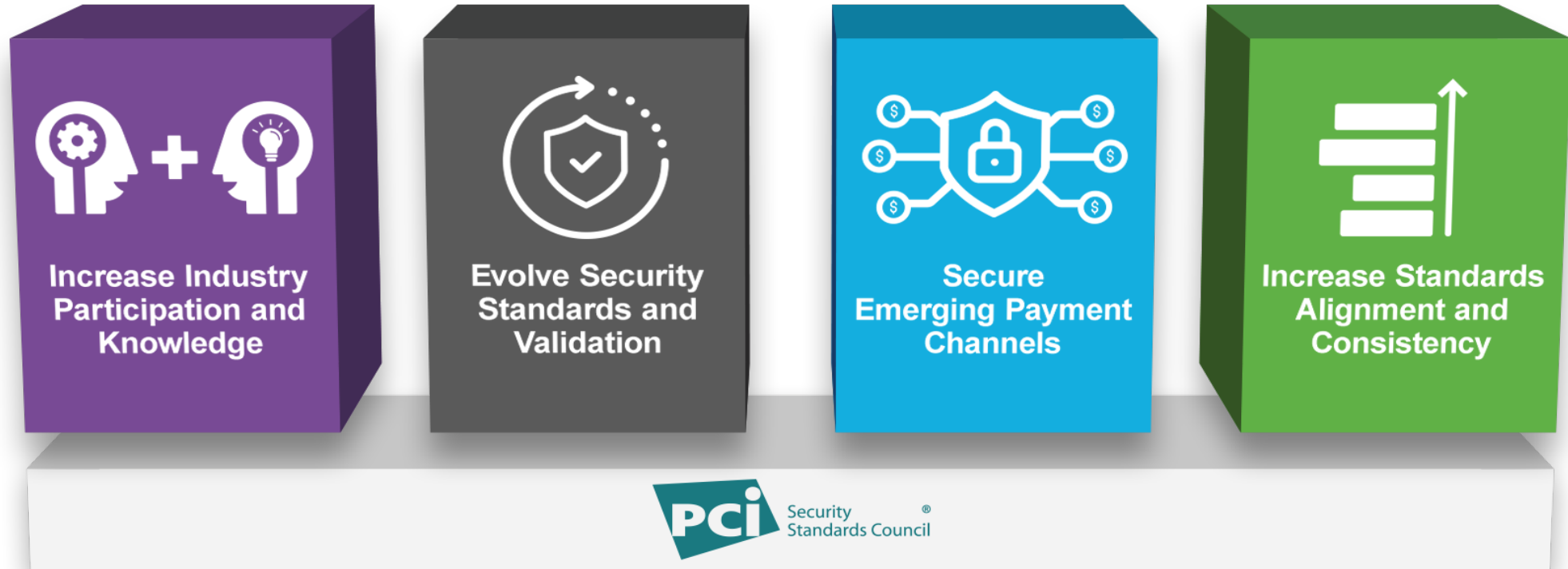
**Global, cross-industry effort to increase  
payment security**

**Industry-driven, flexible and effective  
standards and programs**

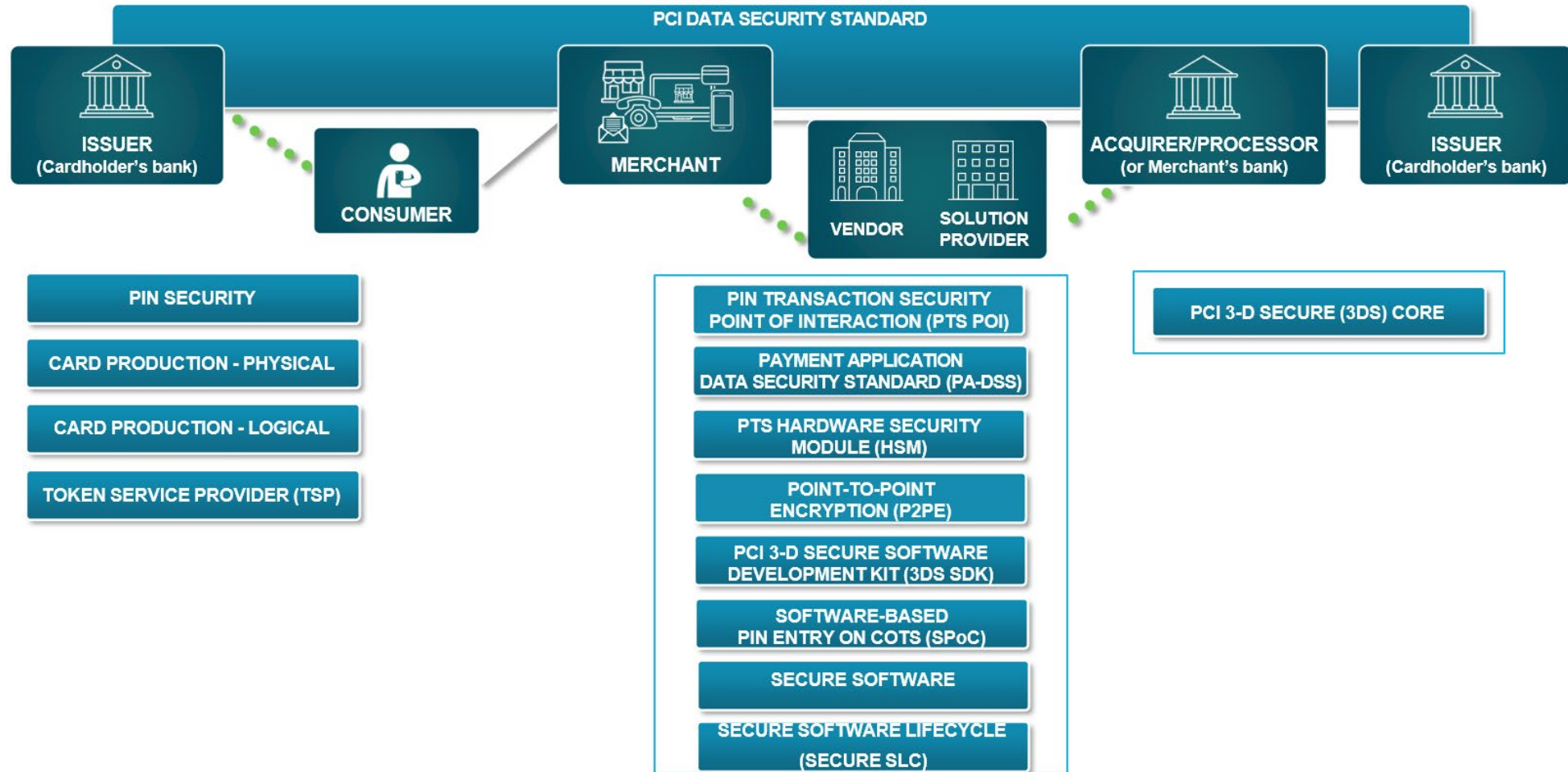
**Helping businesses detect, mitigate and  
prevent criminal attacks and breaches**

# 3. Four Pillar of Activity

[https://www.pcisecuritystandards.org/get\\_involved/participating\\_organizations](https://www.pcisecuritystandards.org/get_involved/participating_organizations)

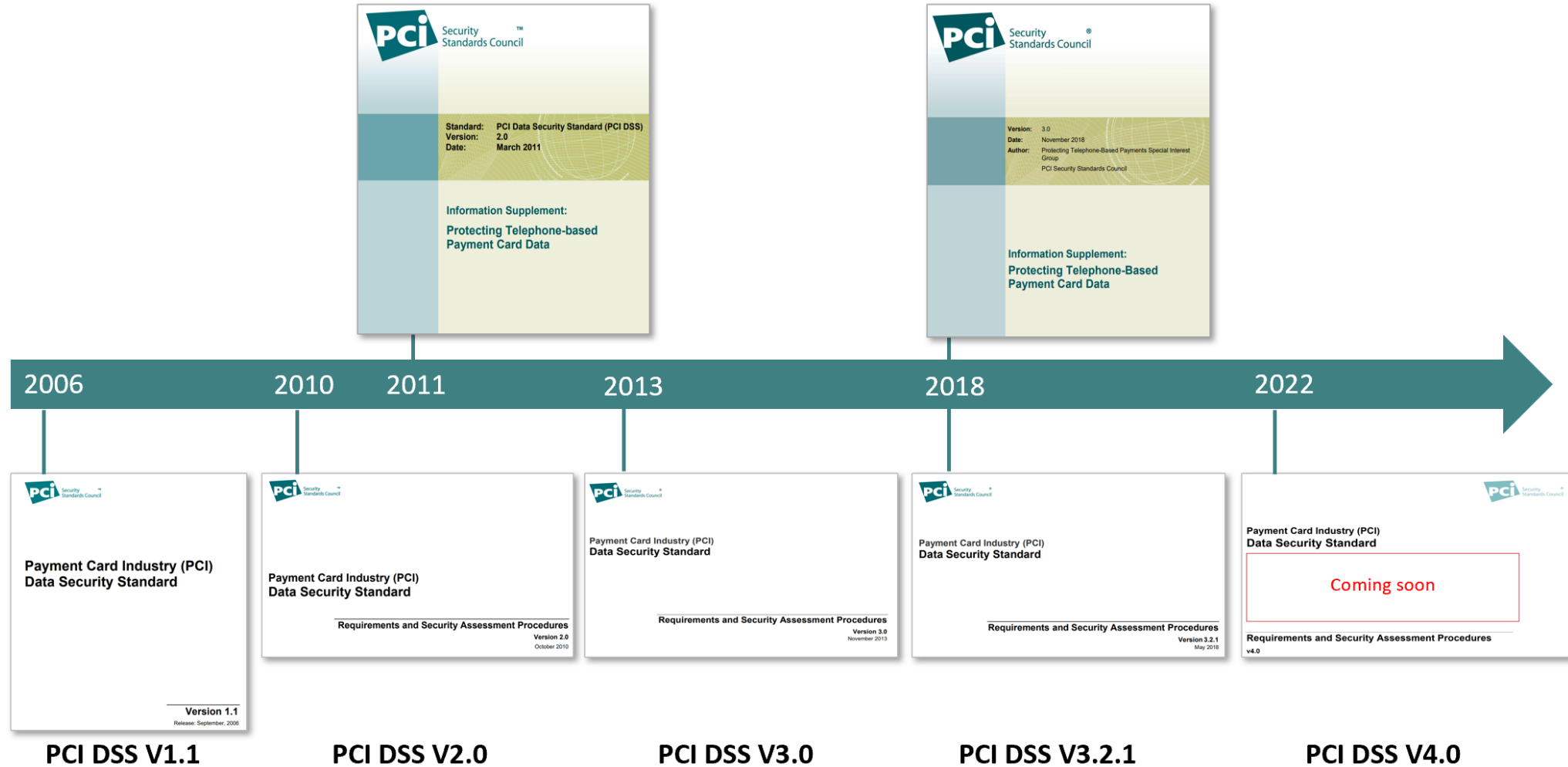


# 4. Fourteen International Standards





# 5. Evolution of the PCI DSS



# 6. The PCI DSS v3.2.1

[https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2-1.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf)



The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to **all** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to **all** other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Below is a high-level overview of the 12 PCI DSS requirements.

## PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network and Systems</b>	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
<b>Protect Cardholder Data</b>	<ol style="list-style-type: none"><li>3. Protect stored cardholder data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"><li>5. Protect all systems against malware and regularly update anti-virus software or programs</li><li>6. Develop and maintain secure systems and applications</li></ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"><li>7. Restrict access to cardholder data by business need to know</li><li>8. Identify and authenticate access to system components</li><li>9. Restrict physical access to cardholder data</li></ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
<b>Maintain an Information Security Policy</b>	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security for all personnel</li></ol>




# 7. Relationship to data protection

[https://icosearch.ico.org.uk/s/search.html?query=pci+dss&collection=ico-meta&profile=\\_default](https://icosearch.ico.org.uk/s/search.html?query=pci+dss&collection=ico-meta&profile=_default)



## Example

If you are processing payment card data, you are obliged to comply with the [Payment Card Industry Data Security Standard](#) . The PCI-DSS outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the UK GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

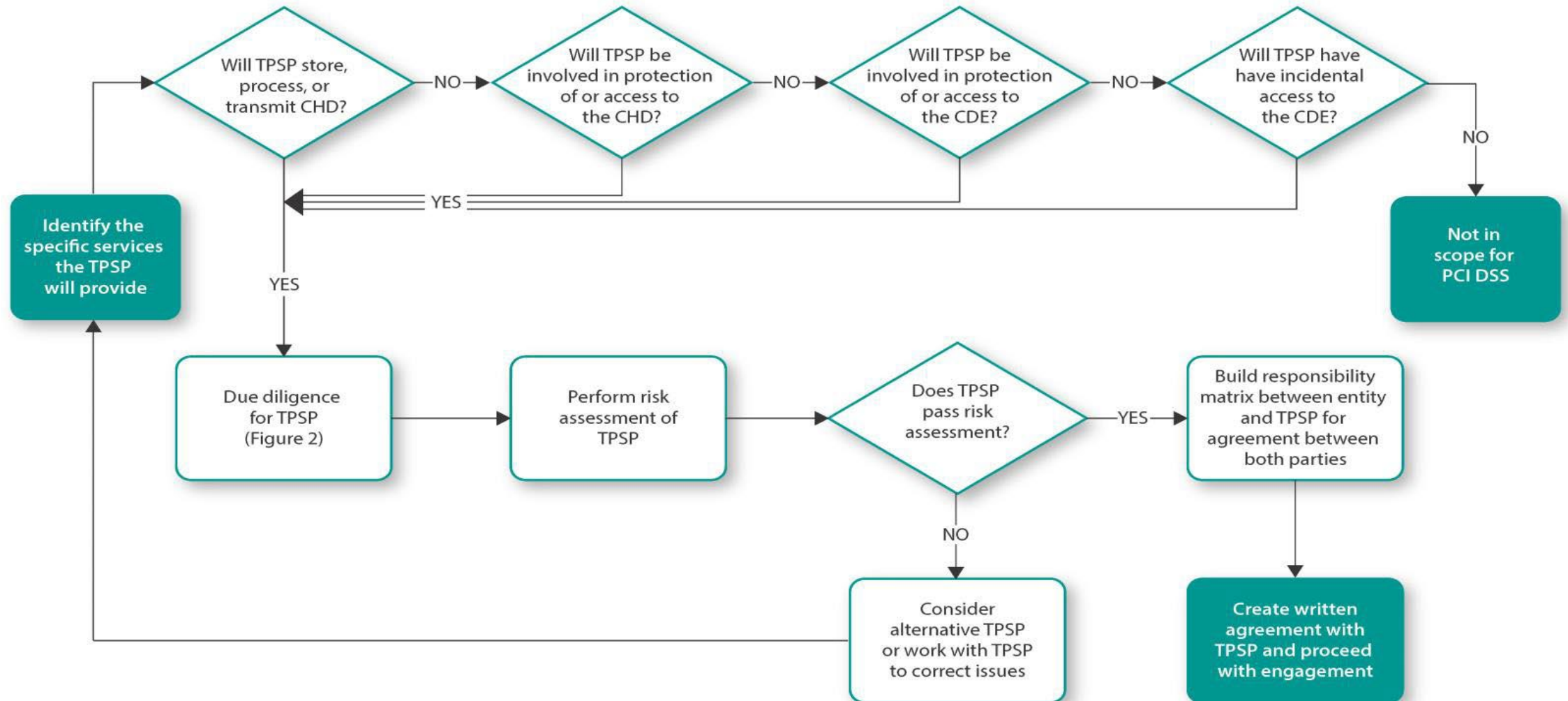
## 8. Definitions – TPSP

*Third Party Service Provider (TPSP) definition. Page 13.*

*A business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. **This also includes companies that provide services that control or could impact the security of cardholder data.** Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. **If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).***

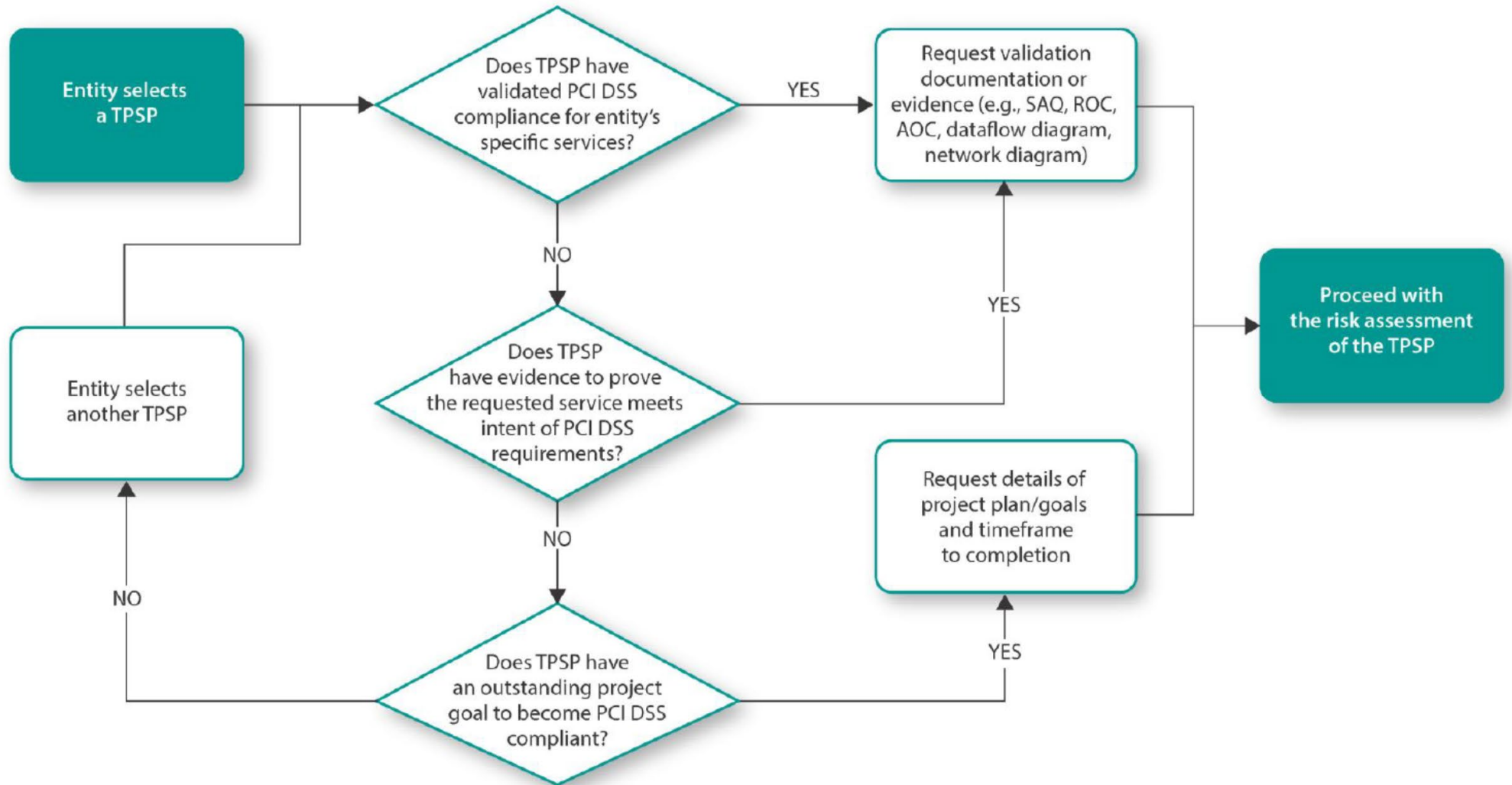
# 9. Third Party Assurance

(March 2016 – Figure 1 High-level TPSP Engagement Process)



# 10. Third Party Assurance

(March 2016 – Figure 2 Example of due-diligence process)



# 11. PCI DSS Requirement 12.8

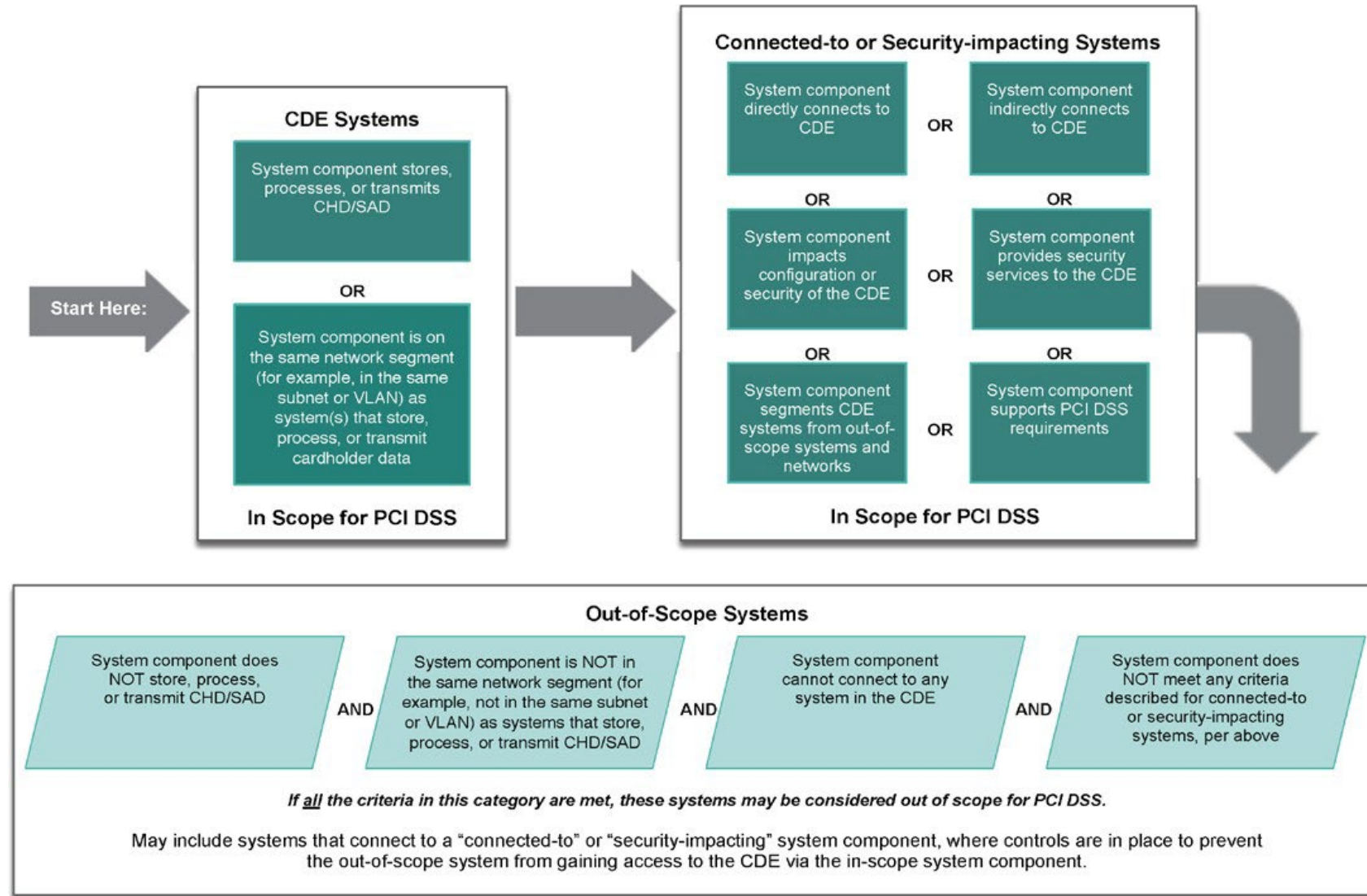


<b>Maintain an Information Security Policy</b> <b>Requirement 12: Maintain a policy that addresses information security for all personnel</b> <i>Note: For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.</i>		
	PCI DSS Question	Expected Testing
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	§ Review policies and procedures. § Observe processes. § Review list of service providers.
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?  <i>Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</i>	§ Observe written agreements. § Review policies and procedures.
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	§ Observe processes. § Review policies and procedures and supporting documentation.
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	§ Observe processes. § Review policies and procedures and supporting documentation.
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	§ Observe processes. § Review policies and procedures and supporting documentation.
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	§ Review the incident response plan. § Review incident response plan procedures.



# 12. Guidance on scoping

(May 2017 – Figure 1 PCI DSS Scoping Categories)





# 13. SAQ's applicable to contact centres

[https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3\\_2\\_1.pdf?agreement=true&time=1642398801609](https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2_1.pdf?agreement=true&time=1642398801609)

Telephone Environments					SAQ Applicability
Merchant SAQ	Payment Channels	Requirements & Controls	PCI SSC Guidance Summary Descriptive Text		
A	MOTO & ECOMM	5 Requirements & 25 Controls	Card-not-present merchants that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.		Applicable <u>ONLY</u> to telephone environment with no CDE or otherwise agreed directly with the merchants acquirer. Which means no cardholder data stored, processed <u>or transmitted</u> , with appropriate controls in place for unintentional card data. <u>Technology deployed to ensure no spoken account data transmitted within merchant environment.</u>
C	MOTO & ECOMM	12 Requirements & 105 Controls	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.		Applicable to telephone environments with a limited CDE (e.g. spoken payment card data or unflattended DTMF tones bringing telephone infrastructure into scope) and NO payment card data stored in business applications, call recordings, web chat or social media systems.
C-VT	MOTO & ECOMM	10 Requirements & 66 Controls	Merchants who <u>manually enter a single transaction at a time via a keyboard into an internet-based, virtual payment terminal</u> solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.		Applicable <u>ONLY</u> to small merchants (typically Level 4) <u>who manually enter a single transaction at a time via a keyboard into an internet-based virtual terminal solution.</u> Developed specifically for small businesses. NOT APPLICABLE to contact centres.
D	ALL CHANNELS	12 Requirements & 329 Controls	All merchants not included in descriptions for any other SAQ		Applicable to contact centres with a CDE (e.g. spoken payment card data or unflattended DTMF tones bringing telephony infrastructure and connected systems into scope) with payment card data stored in business applications, call recordings, web chat or social media applications.

# 14a. SAQ A for contact centres – No spoken CHD

## 25 Controls across 5 PCI DSS Requirements.

Applies when all payment card functions outsourced. No spoken payment card data in the merchant environment.

<p>Requirement 1</p> <p>Install and maintain a firewall configuration to protect cardholder data</p>	<p>Requirement 2</p> <p>Do not use vendor-supplied defaults for system passwords and other security parameters</p>	<p>Requirement 3</p> <p>Protect stored cardholder data</p>	<p>Requirement 4</p> <p>Encrypt transmission of cardholder data across open, public networks</p>	<p>Requirement 5</p> <p>Use and regularly update anti-virus software</p>	<p>Requirement 6</p> <p>Develop and maintain secure systems and applications</p>
<p>Requirement 7</p> <p>Restrict access to cardholder data by business need-to-know</p>	<p>Requirement 8</p> <p>Assign a unique ID to each person with computer access</p>	<p>Requirement 9</p> <p>Restrict physical access to cardholder data</p>	<p>Requirement 10</p> <p>Track and monitor all access to network resources and cardholder data</p>	<p>Requirement 11</p> <p>Regularly test security systems and processes</p>	<p>Requirement 12</p> <p>Maintain a policy that addresses information security</p>

N/A when no access to CHD exists and no media stored reducing to 1 Requirements and 6 Controls

# 14b. SAQ A qualification criteria



## Before You Begin

SAQ A has been developed to address requirements **applicable to merchants whose cardholder data functions are completely outsourced to validated third parties**, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

**SAQ A merchants confirm that, for this payment channel:**

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions
- All processing of cardholder data **is entirely outsourced to PCI DSS validated third-party service providers**
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions
- **Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant** and
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

# 15. SAQ C for contact centres – Spoken CHD

## 105 Controls across all 12 PCI DSS Requirements.

Applies to merchants using a virtual terminal with agents listening to spoken payment card data. Applies when merchants have deployed pause & resume tech' - which only takes call recorder & recording storage out of scope.

### Requirement 1

Install and maintain a firewall configuration to protect cardholder data

### Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

### Requirement 3

Protect stored cardholder data

### Requirement 4

Encrypt transmission of cardholder data across open, public networks

### Requirement 5

Use and regularly update anti-virus software

### Requirement 6

Develop and maintain secure systems and applications

### Requirement 7

Restrict access to cardholder data by business need-to-know

### Requirement 8

Assign a unique ID to each person with computer access

### Requirement 9

Restrict physical access to cardholder data

### Requirement 10

Track and monitor all access to network resources and cardholder data

### Requirement 11

Regularly test security systems and processes

### Requirement 12

Maintain a policy that addresses information security

# 16. SAQ D SP for TPSP – Spoken CHD

## 356 Controls across all 12 PCI DSS Requirements.

Applies to all Third Party Service Providers. Applies when spoken or typed cardholder account data is transmitted across the entities infrastructure i.e. when a Cardholder Data Environment exists.

### Requirement 1

Install and maintain a firewall configuration to protect cardholder data

### Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

### Requirement 3

Protect stored cardholder data

### Requirement 4

Encrypt transmission of cardholder data across open, public networks

### Requirement 5

Use and regularly update anti-virus software

### Requirement 6

Develop and maintain secure systems and applications

### Requirement 7

Restrict access to cardholder data by business need-to-know

### Requirement 8

Assign a unique ID to each person with computer access

### Requirement 9

Restrict physical access to cardholder data

### Requirement 10

Track and monitor all access to network resources and cardholder data

### Requirement 11

Regularly test security systems and processes

### Requirement 12

Maintain a policy that addresses information security

# 17. Visa classifications of TPSP

**Table 1 - Third Party Agent PCI DSS Validation Requirements and Levels**

Level	Service provider	Validation Requirements
1	Visa System Processors <sup>1</sup> or any service provider that stores, processes and/or transmits over 300,000 transactions per year	<ul style="list-style-type: none"><li>▪ Annual Report on Compliance (ROC) by QSA</li><li>▪ Attestation of Compliance (AOC) Form</li></ul>
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	<ul style="list-style-type: none"><li>▪ Annual Self-Assessment Questionnaire (SAQ)</li><li>▪ Attestation of Compliance (AOC) Form</li><li>▪ A passing ASV Executive Summary dated within the last 90 days</li></ul>

<sup>1</sup> A Visa System Processor (VSP) is a member or non-member that has a direct connection to the Visa Europe Authorisation Service.



# 18. Table 5 - Entities in scope

Table 5 – Scope for service providers

Entity	Scenario	In scope for PCI DSS?	Additional factors that may impact scope
Telecommunication companies (telco)	The entity supplies access to public network (analog, digital, and/or IP telephony based), only supporting the point-to-point distribution of call traffic.	Considered out of scope	Some telecommunication equipment owned and operated by the telco, hosted within the entity's infrastructure for the purpose of provisioning access to public network, may be considered in scope for PCI DSS.
One or several service providers (possibly including a telco) providing services such as, for example: IVR, call recording, SIP trunking.	The entities provide a service involving processing, transmitting, or storing account data on behalf of the entity or affecting the security of payment card data.	Considered in scope	<p>The telco or service providers should have their own PCI DSS validation covering the services they provide, or they would need to be included in the entity's PCI DSS assessment.</p> <p>All the relevant service providers should be included in the telephony dataflow.</p> <p>A clear understanding of where the responsibility of each service provider for securing the telephony infrastructure starts and ends, using diagrams that include clearly marked service demarcation points.</p>

# 19. Definitions – TSP



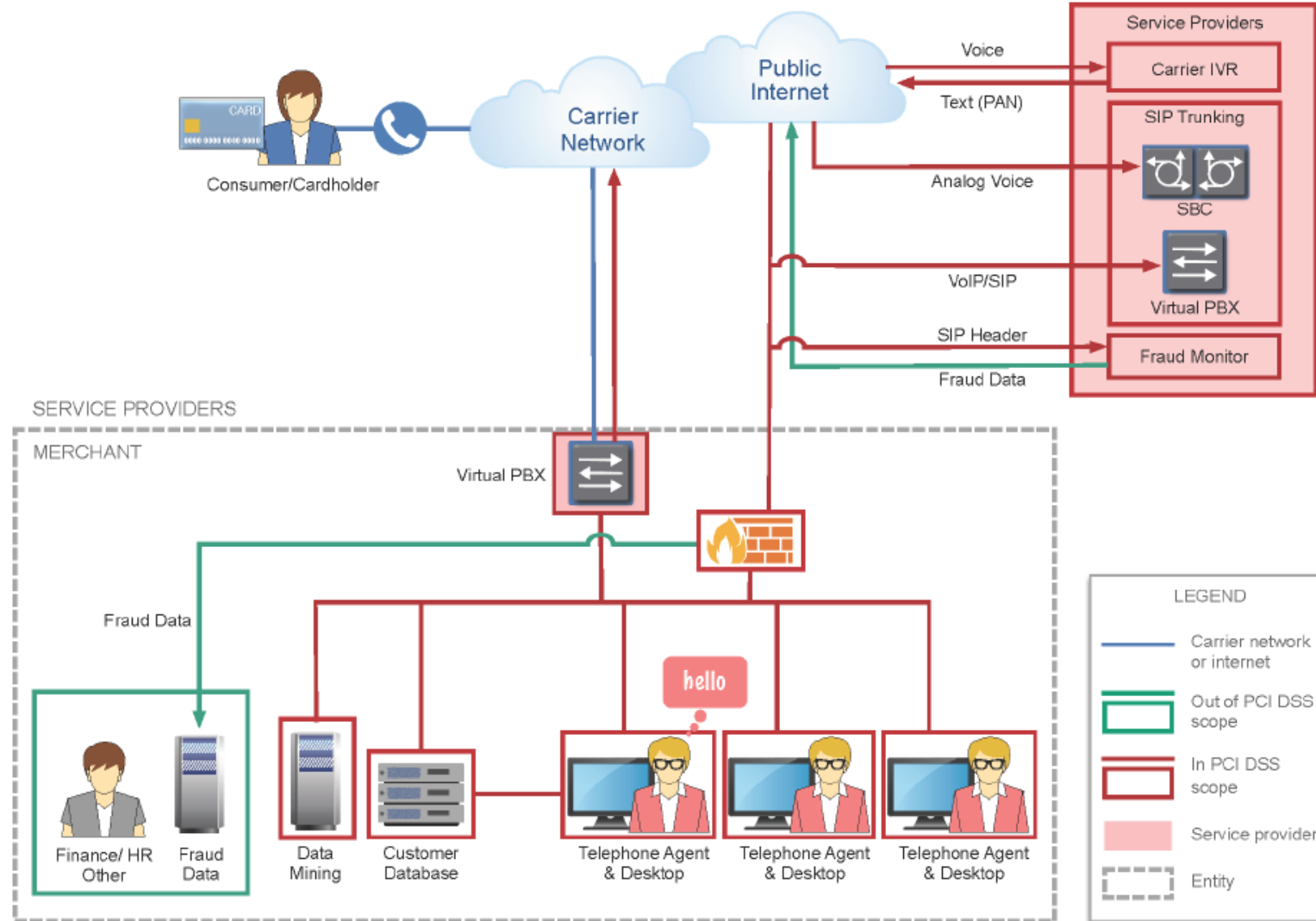
*Telephone Service Provider (TSP) definition. Glossary.*

*Company providing telecommunications services such as telephony and data communications access.*

*Also known as: communication service provider (CSP), digital service provider (DSP), telephone company, telco, or telecommunications operator.*

Includes Unified Communication as a Service (UCaaS) and Contact Centre as a Service (CCaaS)

# 20a. Diagram 6 – Demarcation points



## 20b. Diagram 6 – Demarcation points



Section 2.5 Telephony considerations and demarcation points.

Page 14. Protecting telephone-based card payment data.

Where “voice” traffic from the public telecommunications network (i.e. carrier) terminates on equipment owned and operated by the entity or a service provider and is then sent (regardless of whether it is analog, digital, or VoIP transmission) to a third-party service provider, the demarcation point is the equipment owned by the entity or the third-party service provider and should be considered in scope for PCI DSS.

# 21. Clarity in VoIP – FAQ 1153

<https://www.pcisecuritystandards.org/faqs>



PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted. While PCI DSS does not explicitly reference the use of VoIP, VoIP traffic that contains payment card account data is in scope for applicable PCI DSS controls, just as other IP network traffic containing payment card account data would be. VoIP transmissions originating from an external source and sent to an entity's environment are not considered within the entity's PCI DSS scope until the traffic reaches the entity's infrastructure. This is because an entity cannot control the method of inbound phone calls that their customers and other parties may make, including whether any payment card account data sent over that transmission is being adequately protected by the caller. An entity is considered to have control over the transmission, storage and processing of VoIP traffic within their own network and up to the external perimeter of their infrastructure. The following guidance is intended to assist with PCI DSS scoping for VoIP in different scenarios.

**Internal transmissions:** VoIP traffic containing payment card account data is in scope for applicable PCI DSS controls wherever that traffic is stored, processed or transmitted internally over an entity's network.

**External transmissions to other business entities (business-to-business):** Where an entity uses VoIP for transmission of payment card account data to another business—for example, a service provider or payment processor—the entity's systems and networks used for those transmissions are in scope. Where an entity has end-to-end control over the VoIP connection, the transmission is also in scope for applicable PCI DSS controls. Where an entity cannot control the entire connection—for example, where the transmission passes through multiple telephone carriers between the two entities—the VoIP transmission is within the entity's scope only while the transmission is under control of the entity's infrastructure. This is because the entity does not control how the VoIP traffic will be routed outside of the entity's infrastructure or if all the telephone carriers can support secure connections.

**External transmissions to/from cardholders:** Where VoIP is used for transmissions of payment card account data between a cardholder and an entity, the entity's systems and networks used for those transmissions are in scope. Securing the VoIP transmission outside of the entity's infrastructure is not considered within the entity's scope, as the entity cannot control the methods used by the cardholder to make and receive phone calls. This applies regardless of whether the transmissions are initiated by the entity or the cardholder.

# 22. Diagram 5 – Merchant CDE (Cardholder Data Environment)

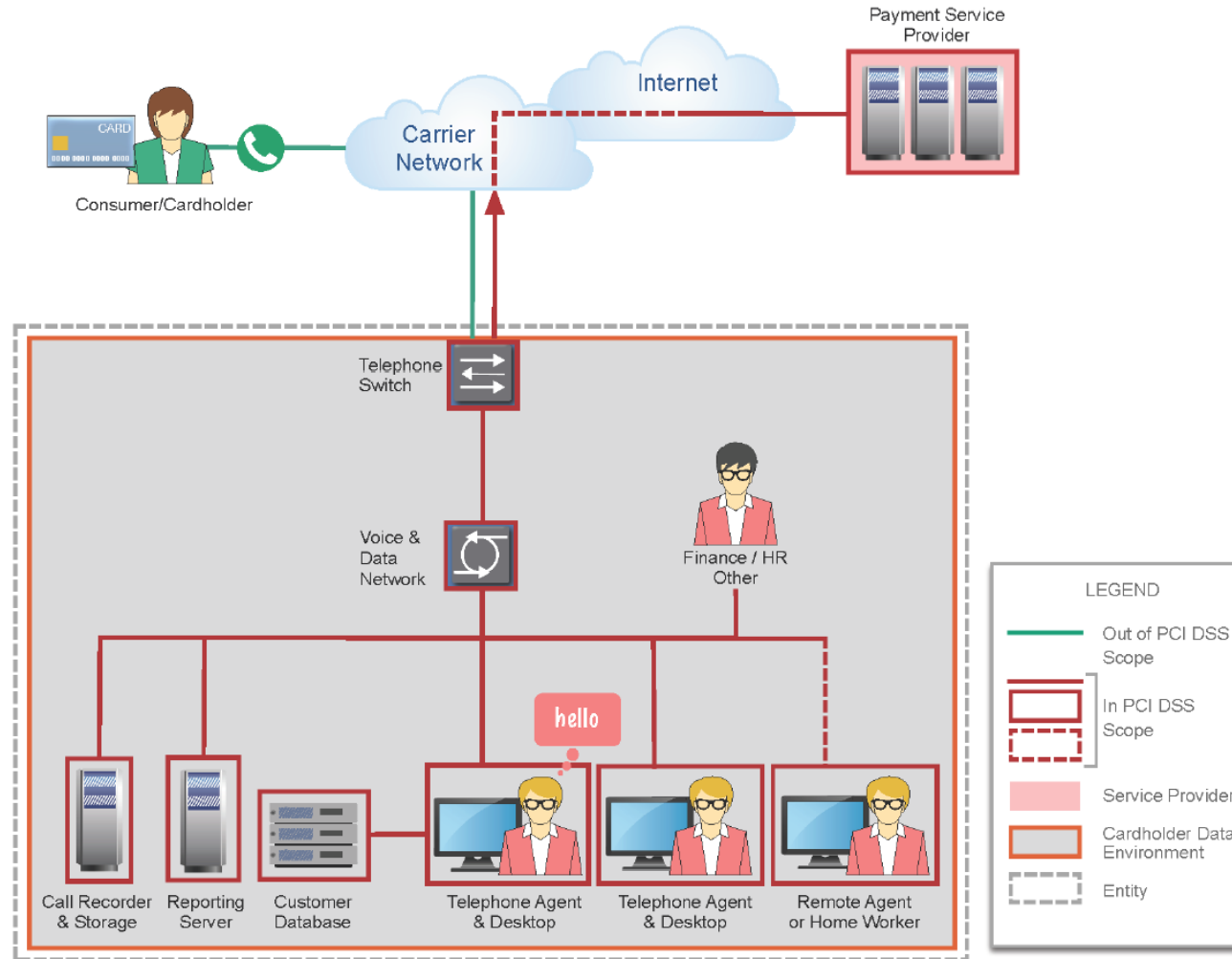
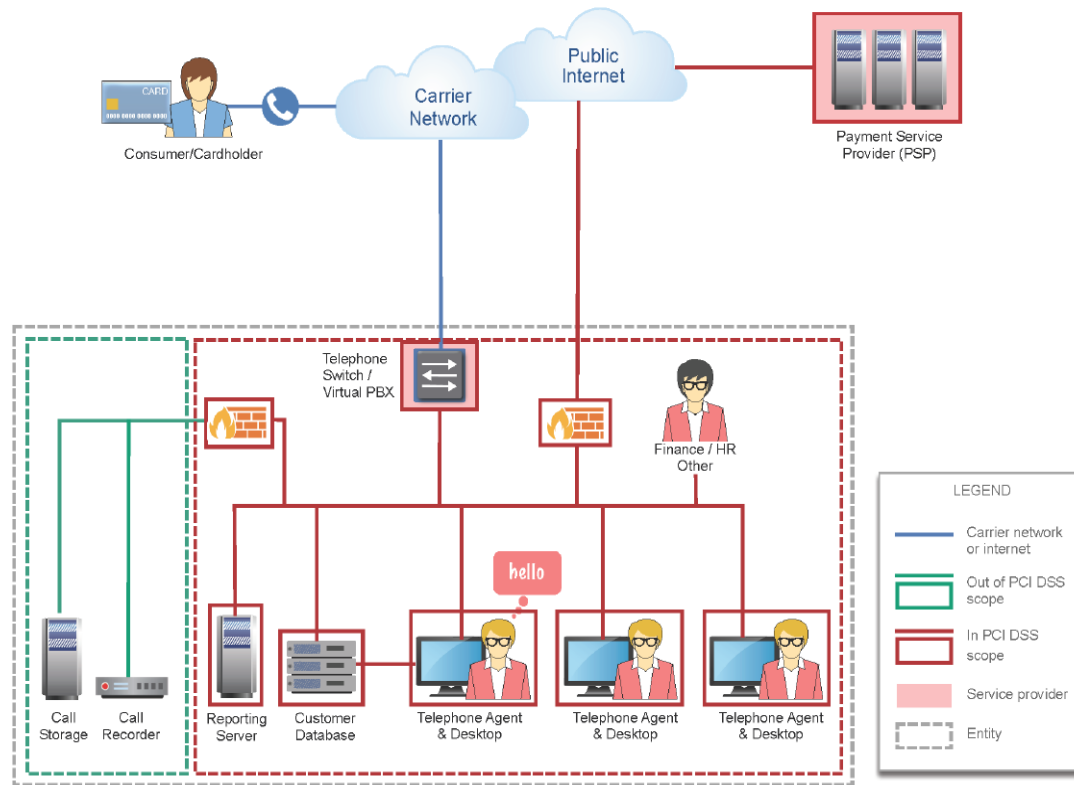


Diagram 5: Cardholder data environment (CDE)



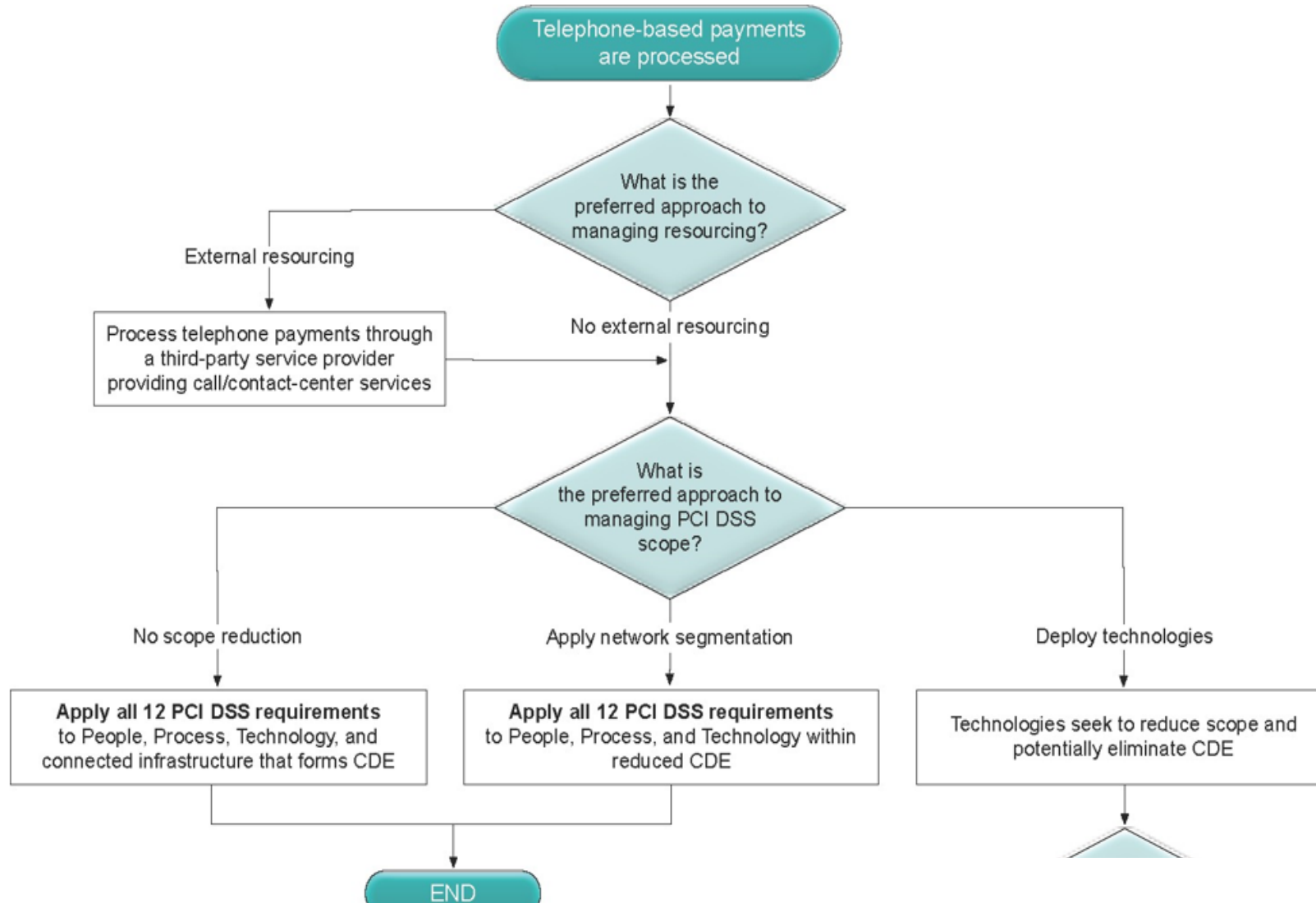
## 23. Diagram 9 - Pause resume



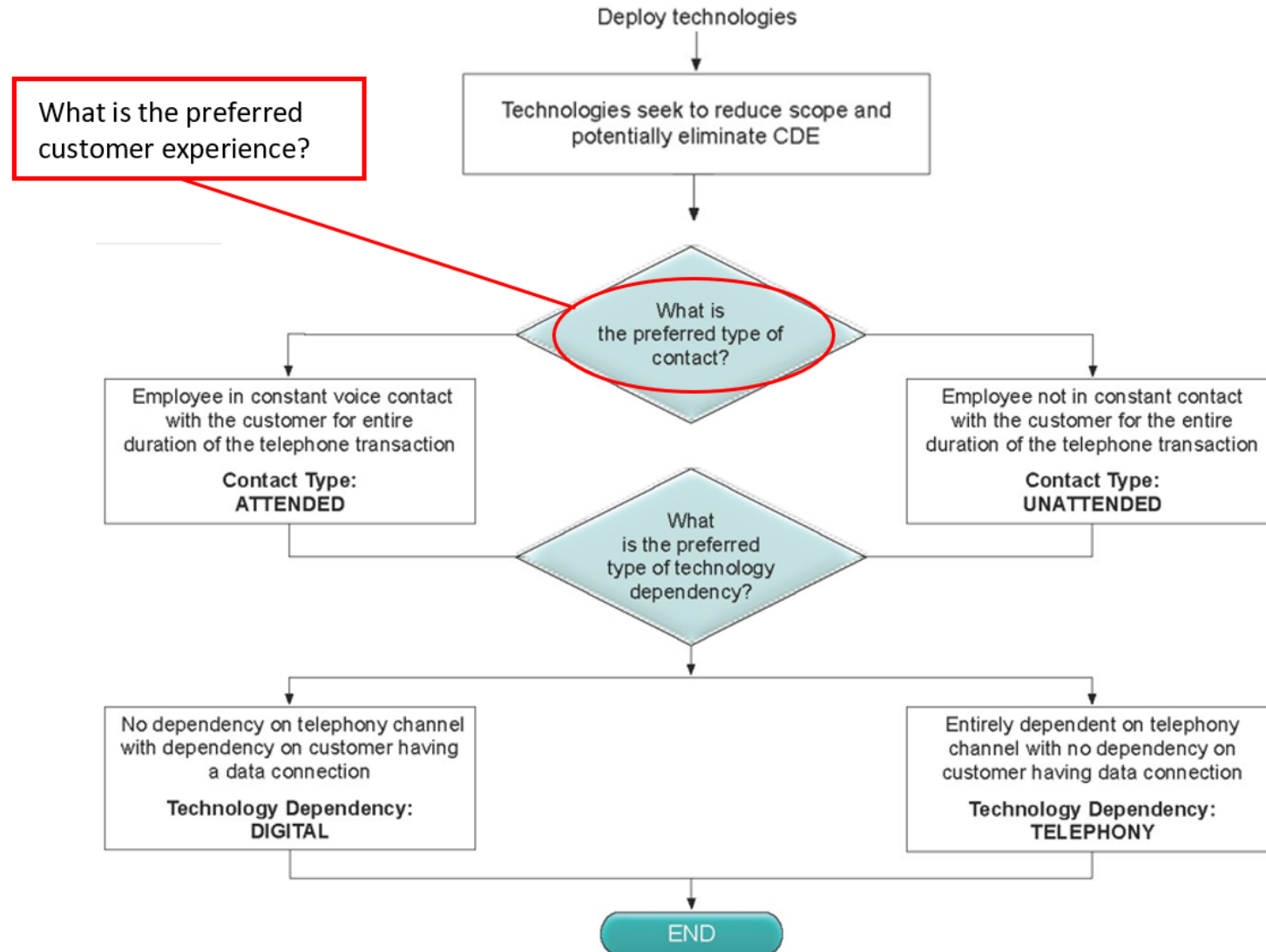
### *Section 6.5. Pause Resume positioning.* Page 36.

*"Pause-and-resume technologies may be manual or automated, and whilst a properly implemented pause-and-resume solution could reduce applicability of PCI DSS by taking the call-recording and storage systems out of scope, the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment as shown in the Diagram 9"*

# 24a. Appendix C – Page 50



# 24b. Appendix C – Page 50



# 25. Technology classifications - examples

## ATTENDED

Agent present for entire duration of the transaction

### TELEPHONY SOLUTIONS

- Network based DTMF – All call traffic
- On-Premis DTMF – All call traffic
- On-Premis DTMF – Payment calls only
- Hosted DTMF – All call traffic
- Hosted DTMF – Payment calls only
- Pause Resume – Manual & Automated

## UNATTENDED

Agent NOT present for entire duration

- Fully automated IVR – Press 1, Press 2
- Automated Voice Recognition / BOT
- Agent pass call to automated IVR to progress payment part of the call without agent present on the call (even if telephony connection remain intact)

### DIGITAL SOLUTIONS

- Agent initiated secure hyperlinks via SMS and / or email
- Agent initiated secure hyperlinks via web chat
- Agent initiated secure hyperlinks via social media

- Embedded secure hyperlinks via electronic documents or email
- Automated secure hyperlinks via SMS and / or email
- BOT driven secure hyperlinks via SMS, chat and / or social media

# 26a. Merchant check list when engaging TPSP

1.

A third party is any entity “that provide services that control or could impact the security of cardholder data”

2.

Listing with Card Brands as a PCI Level 1 compliant service provider

3.

Legal Governance – correct clauses and responsibility matrices, rights to audit and fourth party outsource

4.

Current QSA signed valid Attestations of Compliance that cover “relevant works”

5.

Engaging expert (QSA) support to run pre assessment, reviews of attestation again scope and/or to conduct in **life reviews**

6.

Reading the small print is critical

## 26b. Actions for entities who are TPSP

1.

Understand the TPSP definition. Commit stakeholders to timelines, resources and budgets

2.

Engage specialist expertise to establish a scope reduction strategy, minimising cost, time effort and risk

3.

Review contract terms to enable clients to meet their legal governance obligations

4.

Communicate with clients (merchants) and help them communicate progress to their acquirer

5.

Engage expert support to select appropriate technologies and help select and/or work with your QSA

6.

Turn a cost into a benefit and support your client's data security and PCI DSS compliance obligations.



## 27. Other helpful PCI SSC reference doc's

[ThirdPartySecurityAssurance\\_March2016\\_FINAL.pdf](#)  
([pcisecuritystandards.org](#))

[Protecting\\_Telephone\\_Based\\_Payment\\_Card\\_Data\\_v3-0\\_nov\\_2018.pdf](#)  
([pcisecuritystandards.org](#))

[Protecting Payments While Working Remotely](#) ([pcisecuritystandards.org](#))

FAQ 1494: [For personnel working from home, is the work-from-home environment considered a "sensitive area" for PCI DSS Requirement 9?](#)

FAQ 1495: [Is an assessor required to visit work-from-home environments to determine if personnel are meeting PCI DSS requirements?](#)

FAQ 1496: [Are entities expected to do onsite audits of personnel work-from-home environments?](#)

# 28. Participating organisations

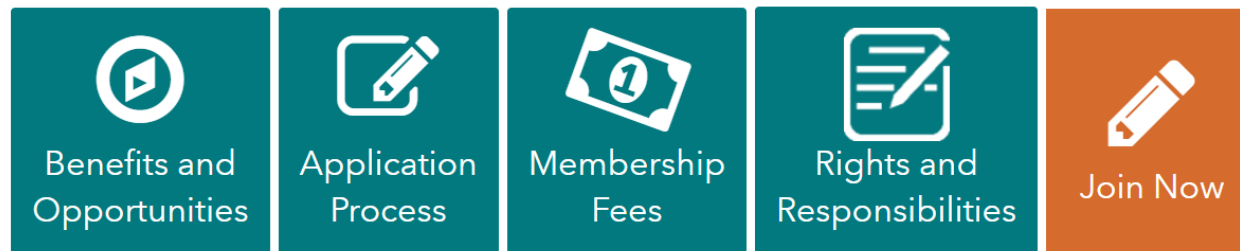
[https://www.pcisecuritystandards.org/get\\_involved/participating\\_organizations](https://www.pcisecuritystandards.org/get_involved/participating_organizations)




Participating Organization membership in the PCI Security Standards Council is open globally to those affiliated with the payment card industry, including merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

Collaboration is at the heart of the Council's mission to help secure payment data globally. As a global forum, we bring together payments industry stakeholders to develop and drive implementation of data security standards and resources for safe payments worldwide.

Join our growing community of Participation Organizations and play an active part in helping secure the future of payments.





If you have any questions about the content within these slides or would like to discuss your payment security requirements contact :-

[john.greenwood@contactcentrepanel.com](mailto:john.greenwood@contactcentrepanel.com)

[www.contactcentrepanel.com](http://www.contactcentrepanel.com)

