支付卡產業 (PCI)
資料安全標準
自我評估問卷

說明與準則

3.2.1 版

2018 年 6 月

文件變更

日期	版本	描述
2008 年 10 月 1 日	1.2	根據新的 PCI DSS 1.2 版調整相關內容，並實施自原始 1.1 版以來所註明的些許變更。
2010 年 10 月 28 日	2.0	根據新的 PCI DSS 2.0 版調整相關內容，並闡明 SAQ 環境類型和資格標準。 為使用 Web 版之虛擬終端機的商家新增 SAQ C-VT
2012 年 6 月	2.1	新增 SAQ P2PE-HW，其適用的商家在處理持卡人資料時，僅使用 PCI SSC 清單上所列之經驗證的「點對點加密」(P2PE) 解決方案包含的硬體終端機。 本文件適用於 PCI DSS 2.0 版。
2015 年 4 月	3.1	根據 PCI DSS 3.1 版調整相關內容，包括新增 SAQ A-EP 與 B-IP，並闡明現有 SAQ 的資格標準。
2016 年 5 月	3.2	更新內容以符合 PCI DSS 3.2 版，並闡明現有 SAQ 的資格標準。
2018 年 6 月	3.2.1	進行些許更新以符合 PCI DSS 3.2.1 版。

确认通知：在所有使用目的和情况下，PCI SSC 网站上的英文文本应作为此文件的官方版本。当翻译文本和英文文本之间出现任何歧义和不一致之处时，正确的内容应以该位置的英文文本为准

目錄

文件變更 ..... **i**

關於本文件 **3**

PCI DSS 自我評估：整體架構 **4**

SAQ 概要 **5**

遵從 PCI DSS 的重要性 **6**

瞭解合規與安全之間的差異 7

符合 PCI DSS 規範的一般提示與策略 7

選擇最適合您組織的 SAQ 和證明 **10**

SAQ A – 採用無卡支付的商家，所有持卡人資料功能全數委外 9

SAQ A-EP – 使用第三方網站將部分付款處理事宜委外的電子商務商家 13

SAQ B – 僅使用刷卡機或獨立撥出終端機，而且不會儲存電子格式的持卡人資料的商家 14

SAQ B-IP – 使用以 IP 連線之 PTS 獨立互動點 (POI) 終端機，而且不儲存電子格式持卡人資料的商家 15

SAQ C-VT – 使用 Web 版虛擬終端機，而且不會儲存電子格式持卡人資料的商家 16

SAQ C – 支付應用系統連接到網際網路，而且不儲存電子格式持卡人資料的商家 17

SAQ P2PE – 僅使用PCI SSC 清單上 P2PE 解決方案 所管理的硬體付款終端機，而且不儲存電子格式持卡人資料的商家 18

商家適用的 SAQ D– 其他所有符合 SAQ 資格條件的商家 19

服務供應商適用的 SAQ D– 符合 SAQ 資格條件的服務供應商 19

哪種 SAQ 最適合我的環境？ **20**

關於本文件

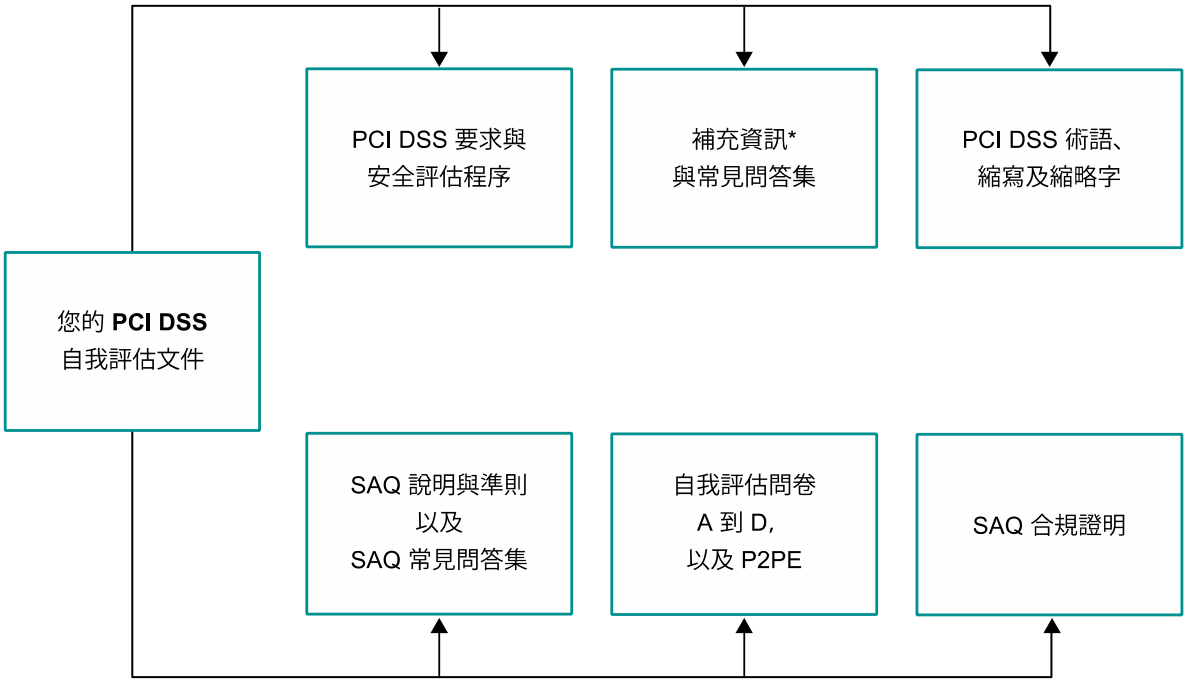
本文件旨在協助商家與服務供應商瞭解支付卡產業資料安全標準 (PCI DSS) 和自我評估問卷 (SAQ)。我們建議您詳細檢閱全部的說明和指南文件，瞭解 PCI DSS 對您組織的重要性，您的組織可使用何種策略促進 PCI DSS 合規性驗證，以及您的組織具備完成哪一個精簡版 SAQ 的資格條件。

PCI DSS 自我評估：整體架構

PCI DSS
與支援文件為一組通用的產業工具，能協助組織確保處理持卡人資料時的安全性。該標準提供了一個可行**的框架，可用於開發健全的帳**戶資料安全程序
(包括預防、偵測和回應安全事故)。為降低資料外洩風險及減輕其造成的影響，所有儲存、處理或傳輸持卡人資料的實體都必須遵守該標準。

下圖列出了一些可以幫助組織達成 PCI DSS 合規和完成自我評估的工具。

這些工具以及其他相關文件可以從以下位址找到：www.pcisecuritystandards.org。



** 附註：「補充資訊」只做為提供補充資訊與指引只用，不能取代 PCI DSS 中的任何要求。*

SAQ 概要

PCI DSS 自我評估問卷 (SAQ) 是一種驗證工具，可以幫助商家與服務供應商對 PCI DSS 的合規性狀況進行自我評估。PCI DSS SAQ 有多個版本，可以滿足各種不同的情況。本文件能協助貴組織判斷哪種 SAQ 最適合貴組織的環境。

PCI DSS SAQ 是一種驗證工具，適用於收單機構或支付品牌未要求提交 PCI DSS 合規性報告 (ROC) 的商家與服務供應商。如需 PCI DSS 驗證要求的詳細資料，請洽詢貴組織的收單機構或支付品牌。

每個 PCI DSS SAQ 均包含以下項目：

1. 與 PCI DSS 要求相關的問題，其適用範圍因商家環境而定：請參閱本文件的「選擇最適合您組織的 SAQ 和證明」。該小節另有基於 PCI DSS 測試程序的「預期測試」欄位。
2. 合規證明：證明包含完成適當 SAQ 的資格宣告，以及 PCI DSS 自我評估的後續結果。

遵從 PCI DSS 的重要性

PCI 安全標準委員會的創始成員 (American Express、Discover、JCB、Mastercard 和 Visa) 一直在監控各種帳戶資料外洩風險。資料外洩風險可能會影響各種類型的組織，從小規模至大規模的商家及服務供應商均有涉及。

安全性缺口和後續的支付卡資料外洩風險會對受害組織造深遠的影響，包括：

1. 監管通知要求、
2. 商譽損失、
3. 客戶流失、
4. 潛在的財務責任 (如監管與其他費用和罰金)，以及
5. 訴訟。

針對資料外洩風險的分析顯示 PCI DSS 雖已給出處理一般安全漏洞的對策，但在實際發生資料外洩時組織並未能執行到位，抑或執行不善。正因為如此，我們才制定了 PCI DSS 和各項詳細規範，目的是盡可能降低發生資料外洩的機率並減輕該情況發生時所造成的影響。

常見 PCI DSS 管控措施失效的範例包括 (但不限於)：

- 在授權後儲存敏感驗證資料 (SAD)，如磁條資料 (規範 3.2)。衆多受威脅的實體並未意識到其系統正在儲存此類資料。
- 因銷售點 (POS) 系統安裝不當，而導致存取控制不足，使惡意使用者可以透過 POS 廠商的路徑入侵 (規範 7.1、7.2、8.2 和 8.3)
- 安裝系統時未變更預設系統設定和密碼 (規範 2.1)。
- 安裝系統時未移除或修復非必要和不安全的服務 (規範 2.2.2 和 2.2.3)。
- 編碼不良的網頁應用程式會導致 SQL 插入和其他漏洞，這些漏洞允許直接從網站存取儲存持卡人資料的資料庫 (規範 6.5)。
- 未進行安全修補及安全修補程式已過期 (規範 6.2)。
- 缺少記錄 (規範 10)。
- 缺少監控 (透過記錄審查、入侵偵測/預防、季度漏洞掃描和變更偵測機制) (規範 10.6、11.2、11.4 和 11.5)。
- 不夠周密的範圍規劃決策。例如，因不當的網路區段劃分，將未經驗證是否有效的部分網路排除在 PCI DSS 範圍之外。(規範 11.3.4)。網路中其他未根據 PCI DSS 安全處理的部分弱點會使持卡人資料環境在不知情的情況下暴露於風險中 (例如，來自不安全的無線存取點，以及透過員工電子郵件和網路瀏覽引入的漏洞) (規範 1.2、1.3 及 1.4）。

瞭解合規與安全之間的差異

組織務必瞭解合規與安全之間的差異。僅在特定時間點符合 PCI DSS 規範，並不能防止環境的情況改變。也就是說，如果組織未實施適當的管控措施，安全性可能會受到影響。因此，您應該確保 PCI DSS 控制作為常規業務 (BAU) 活動的一部分，並按照總體安全策略的定義持續正確實施。這能讓您持續監控組織安全控管措施的有效性，並在多次 PCI DSS 評估之間維護符合 PCI DSS 規範的環境。如需有關將 PCI DSS 作為常規業務活動的範例，請參閱 PCI DSS 的「將 PCI DSS 作為常規業務活動程序的最佳實務」一節。

此外，PCI DSS 安全規範的目的在於保護支付卡資料，不過貴組織可能會有其他不在 PCI DSS 範圍內的敏感資料與資產需要保護。因此，儘管妥善維護 PCI DSS 合規性確實有助於提升整體安全，仍不應以其取代健全的組織安全計畫。

符合 PCI DSS 規範的一般提示與策略

以下是您在準備 PCI DSS 合規驗證時可以參考的一些提示與策略。這些提示有助於排除非必要之持卡人資料的儲存、將您需要的資料隔離至規定且受控的中央區域，並且能夠允許您限制 PCI DSS 合規驗證的工作範圍。例如，透過刪除不需要的持卡人資料和/或將這些資料隔離在規定的受控區域內，您可以將那些不再儲存、處理或傳輸持卡人資料，而且不再與您的系統相連接的系統與網路，從您的自我評估範圍中刪除。

1. **敏感驗證資料 (包括磁條的完整磁軌內容或晶片上的相同資料、卡片驗證碼和值、PIN 碼及 PIN 區塊)**：

   確認您在授權後*絕對沒有儲存這些資料*：

2. **建議您透過以下問題，詢問您的 POS 廠商有關系統的安全狀況**：

   a. 是否已變更組成 POS 系統的系統與資料庫預設設定和密碼？

   b. 您是否會從遠端存取我的 POS 系統？如果會，您是否已實施了適當的管控措施，以防止他人存取我的 POS 系統？例如，使用安全的遠端存取方法、不使用常見的或預設密碼。您從遠端存取我的 POS 裝置的頻率以及存取的原因？誰有權從遠端存取我的 POS 裝置？

   c. 是否已移除組成 POS 系統的所有非必要和不安全的服務？

   d. 我的 POS 軟體是否通過了支付應用系統資料安全標準 (PA-DSS) 驗證？(請參閱 PCI SSC 的驗證支付應用系統清單。)

   e. 我的 POS 軟體是否會儲存磁條資料或 PIN 區塊等敏感驗證資料？如果會，儲存這些資料是不允許的，那麼您能多快幫我移除這些資料？

   f. 我的 POS 軟體是否會儲存主要帳戶號碼 (PAN)？如果會，此類儲存必須受到保護，那麼 POS 如何保護此類資料？

g. 您是否會記錄關於應用系統所列檔案的清單並概要記錄每個檔案的內容，以驗證是否儲存上述禁止儲存的資料？

h. 存取我的 POS 軟體時是否需要使用複雜與唯一密碼？

i. 您可以確認您未使用常見的或預設的密碼，來存取我的系統以及您支援的其他商家系統嗎？

j. 是否已利用所有適用的安全更新對組成 POS 系統的所有系統和資料庫進行修補？

k. 是否已為組成 POS 系統的系統和資料庫開啟了記錄功能？

l. 如果我以前的 POS 軟體會儲存敏感驗證資料，目前對 POS 軟體的更新是否已經移除此項功能？移除這些資料時是否使用了安全擦除公用程式？

3. 持卡人資料—如果您不需要，請不要儲存！

a. 支付品牌規則允許儲存主要帳戶號碼 (PAN)、到期日、持卡人姓名及服務代碼。

b. 記錄您儲存這些資料的所有原因和地點。如果這些資料不具有合法的業務目的，請考慮刪除。

c. 考量儲存這些資料及其支援的業務流程是否值得付出以下代價：

i. 資料外洩的風險。

ii. 為保護這些資料必須針對 PCI DSS 付出的額外努力。

iii. 為長期符合 PCI DSS 規範需付出的持續性維護成本。

4. 持卡人資料—如果您需要，請將其合併和隔離。

您可以透過在定義環境內合併資料儲存並使用正確的網路區段劃分隔離資料，以限制 PCI DSS 評估的範疇。例如，如果您的員工瀏覽網際網路或接收電子郵件是與持卡人資料使用同一機器或網路區段，請考慮劃分 (隔離) 持卡人資料到其自有機器或網路區段 (例如，透過路由器或防火牆)。如果您能有效隔離持卡人資料，則僅須專注於隔離部分的 PCI DSS 合規性，而不必關注所有的機器。

5. 補償性管控措施

當組織無法滿足特定的技術規範要求，但已透過替代管控措施大幅降低相關風險時，可以考慮使用補償性管控措施來滿足大部分 PCI DSS 規範。如果您的組織沒有採用與 PCI DSS 規範完全相同的控制，但是已制定了符合 PCI DSS「補償性管控」定義的管控措施 (請參閱 PCI DSS 附錄 B 以及 *《PCI DSS 與 PA-DSS 術語、縮寫及縮略字》* 文件中的對「補償性管控」的定義)，則應採取以下行動：

a. 請遵循 PCI DSS 附錄 B 中針對補償性管控措施所列示的程序。

b. 針對在補償性管控措施的支援下滿足的所有要求，請在回答 SAQ 問題時勾選「是，使用 CCW」欄位。

c. 完成 SAQ 附錄 B 的「補償性管控工作表」，記錄每項補償性管控措施的使用狀況。

請務必填寫「補償性管控工作表」，記錄每項透過補償性管控而達成的要求。

d. 根據收單機構或支付品牌的說明，提交所有完成的「補償性管控工作表」以及 SAQ 及/或合規證明。

6. 專業協助與訓練

a. 如果您希望在安全專業人員的協助下完成自我評估，我們建議您考慮聯絡合格安全評估機構 (QSA)。QSA 由 PCI SSC 所訓練，負責進行 PCI DSS 評估，並且列示於 PCI SSC 網站上。

b. PCI SSC 網站是其他資源的主要來源，包括：

- *PCI DSS 術語、縮寫及縮略字*
- 常見問答集 (FAQ)
- 線上研討會
- 補充資訊與準則
- SAQ 表單與合規證明

***附註：**「補充資訊」是 PCI DSS 的補充材料，同時提供滿足 PCI DSS 規範的額外考量因素與建議事項，但不會變更、消除或取代 PCI DSS 規範或其中任何內容。*

c. PCI SSC 另提供一些訓練計畫，能協助組織的相關人員培養安全意識。相關訓練包括「PCI 安全意識訓練」、「PCI 專業人員」(PCIP) 計畫，以及「內部安全評估員」(ISA) 計畫。

如需詳細資訊，請參閱 www.pcisecuritystandards.org。

d. 支付品牌和/或商家收單機構也可能會提供支付相關的訓練計畫與資源。

選擇最適合您組織的 SAQ 和證明

所有商家和服務供應商都必須始終遵循適用於其環境的 PCI DSS 規範。下表簡單顯示幾種 SAQ 類型，更詳細的描述請參閱後文。使用該表判斷哪種 SAQ 適用於您的組織，然後查閱詳細描述，確保能滿足該 SAQ 的所有要求。

附註 (針對 SAQ D 之外的所有 SAQ)：這些 SAQ 含有適用於特定商家環境類型的問題，如相關 SAQ 資格條件所定義。倘若特定 SAQ 未涵蓋貴組織環境適用的 PCI DSS 要求，代表該 SAQ 可能不適合貴組織的環境。此外，您必須遵循所有適用的 PCI DSS 規範，才能達成 PCI DSS 合規。

SAQ	說明
A	採用無卡支付的商家 (電子商務、郵購/電話訂購)，其將所有持卡人資料處理事宜委外給符合 PCI DSS 規範的第三方服務供應商，而且未在商家的系統或營業場所儲存、處理或傳輸任何電子格式的持卡人資料。 *不適用於面對面付款交易的商家。*
A-EP	採用電子商務的商家，其將所有付款處理作業委外給經 PCI DSS 驗證的第三方服務供應商，而且該商家的網站不會直接收取持卡人資料，因此可能影響付款交易的安全性。這類商家的系統或營業場所不會儲存、處理或傳輸任何電子格式的持卡人資料。 *僅適用於電子商務商家。*
B	僅限使用以下裝置的商家： ▪ 不儲存電子格式持卡人資料的刷卡機，和/或 ▪ 不儲存電子格式持卡人資料的獨立撥出終端機。 *不適用於電子商務商家。*
B-IP	這類商家僅使用經 PTS 核可的獨立付款終端機，並以 IP 連線連接付款處理方，而且不會儲存電子格式的持卡人資料。 *不適用於電子商務商家。*
C-VT	這類商家透過鍵盤手動將交易逐筆輸入網際網路版虛擬付款終端機解決方案，該解決方案由經 PCI DSS 驗證的第三方服務供應商提供及代管，而且不會儲存電子格式的持卡人資料。 *不適用於電子商務商家。*

SAQ	說明
C	這類商家的支付應用系統連接到網際網路，而且不會儲存電子格式持卡人資料。 *不適用於電子商務商家。*
P2PE	這類商家僅使用由經驗證的 PCI SSC 清單所列的「點對點加密」(P2PE) 解決方案所管理的硬體付款終端機；不會儲存電子格式的持卡人資料。 *不適用於電子商務商家。*
D	***商家適用的 SAQ D：***所有不包括在前述 SAQ 類型描述中的商家。
	服務供應商適用的 SAQ D：由支付品牌定義為符合 SAQ 的資格條件的服務提供商。

e. SAQ A – 採用無卡支付的商家，所有持卡人資料功能全數委外

SAQ A
的制定是為了幫助以下商家符合適用規範，這類商家將所有持卡人資料處理事宜委外給第三方服務供應商，僅留存含持卡人資料的書面報告或收據。

SAQ A
適用的商家可能是接受無卡支付的電子商務或郵購/電話訂購商家，而且他們不會在系統或營業場所儲存、處理或傳輸任何電子格式的持卡人資料。

SAQ A 適用的商家必須確認其符合以下針對此支付管道的資格條件：

- 貴公司僅接受無卡支付 (電子商務或郵購/電話訂購) 交易；
- 所有持卡人資料的處理事宜全數委外給經 PCI DSS 驗證的第三方服務供應商；
- 貴公司不在系統或營業場所儲存、處理或傳輸任何電子格式的持卡人資料，而是完全仰賴第三方來處理前述所有事宜；
- 貴公司確認所有負責進行持卡人資料之儲存、處理及/或傳輸事宜的第三方均符合 PCI DSS 規範；**以及**
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件。

此外，針對電子商務商家：

- 所有傳送至消費者瀏覽器之付款頁面的項目，必須由第三方服務供應商直接提供，且該服務供應商必須通過 PCI DSS 驗證。

此 SAQ 不適用於面對面付款交易的商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ A-EP – 使用第三方網站將部分付款處理事宜委外的電子商務商家

SAQ A-EP
的制定是為了幫助以下電子商務商家符合適用規範，這類商家的網站不直接收取持卡人資料，因此可能影響付款交易的安全性，以及/或收取消費者持卡人資料頁面的完整性。

SAQ A-EP 適用的商家為電子商務商家，這類商家將部分的電子商務支付管道委外給經 PCI DSS 驗證的第三方服務供應商處理，而且不會在系統或營業場所儲存、處理或傳輸任何電子格式的持卡人資料。

SAQ A-EP 適用的商家必須確認其符合以下針對此支付管道的資格條件：

- 貴公司僅接受電子商務交易；
- 除了付款頁面之外，所有持卡人資料的處理事宜全數委外給經 PCI DSS 驗證的第三方服務供應商；
- 您的電子商務網站不會收取持卡人資料，但是會控制網站如何將消費者或其持卡人資料重新導向經過 PCI DSS 驗證的第三方服務供應商。
- 如果您的網站是由第三方供應商代管，則該供應商必須通過所有適用的 PCI DSS 規範的驗證 (例如，如果供應商是共享代管供應商，還必須通過 PCI DSS 附錄 A 的規範)。
- 每個傳送至消費者瀏覽器之付款頁面的項目，均來自商家網站或符合 PCI DSS 規範的服務供應商。
- 貴公司不在系統或營業場所儲存、處理或傳輸任何電子格式的持卡人資料，而是完全仰賴第三方來處理前述所有事宜；
- 貴公司確認所有負責進行持卡人資料之儲存、處理及/或傳輸事宜的第三方均符合 PCI DSS 規範；**以及**
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件。

此 SAQ 僅適用於電子商務商家。

附註：*為達成 SAQ A-EP 的目的，「持卡人資料環境」適用的 PCI DSS 要求同樣適用於商家網站。這是因為即使商家網站本身不收取持卡人資料，還是會直接影響支付卡資料的傳輸方式。*

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ B –

僅使用刷卡機或獨立撥出終端機，而且不會儲存電子格式的持卡人資料的商家

SAQ B
的制定是為了幫助以下電子商務商家符合適用規範，這類商家僅透過刷卡機或獨立撥出終端機處理持卡人資料。

SAQ B 適用的商家可以是實體 (出示實卡) 或郵購/電話訂購 (無卡支付)
的商家，而且不會將持卡人資料儲存在任何電腦系統上。SAQ B
適用的商家必須確認其符合以下針對此支付管道的資格條件：

- 貴公司只使用刷卡機和/或獨立撥出終端機 (透過電話線連接處理方) 提取客戶的支付卡資訊；
- 獨立撥出終端機未連接貴公司環境內的其他任何系統；
- 獨立撥出終端機未連接網際網路；
- 貴公司不透過網路 (內部網路或網際網路) 傳輸持卡人資料；
- 貴公司留存的所有持卡人資料均為紙本形式
  (如列印的報告或收據)，而且不會透過電子方式接收這些文件；**以及**
- 貴公司不儲存電子格式的持卡人資料。

此 SAQ 不適用於電子商務商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ B-IP – 使用以 IP 連線之 PTS 獨立互動點 (POI) 終端機，而且不儲存電子格式持卡人資料的商家

SAQ B 的制定是為了幫助以下商家符合適用規範，這類商家在處理持卡人資料時，僅使用經 PTS 核可的獨立互動點 (POI) 裝置，並以 IP 連接付款處理方。

SAQ B-IP 適用的商家可以是實體 (出示實卡) 或郵購/電話訂購 (無卡支付) 的商家，而且不會將持卡人資料儲存在任何電腦系統上。

SAQ B-IP 適用的商家必須確認其符合以下針對該支付管道的資格條件：

- 貴公司只使用經 PTS 核可的獨立互動點 (POI) 裝置 (不包括 SCR)，並透過 IP 連接付款處理方之方式提取客戶的支付卡資訊。
- 透過 IP 連線的獨立 POI 裝置已驗證符合 PCI SSC 網站列舉的 PTS POI 計畫 (不包括 SCR)；
- 透過 IP 連線的獨立 POI 裝置未連接貴公司環境內的其他任何系統 (可以透過網路區段劃分將 POI 裝置與其他系統隔離來達成)。
- 僅允許將持卡人資料從經 PTS 核可的 POI 裝置傳輸至付款處理方；
- POI 裝置連接付款處理方時，不用透過任何其他裝置 (如電腦、行動電話、平板電腦等)；
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件；**以及**
- 貴公司不儲存電子格式的持卡人資料。

此 SAQ 不適用於電子商務商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ C-VT – 使用 Web 版虛擬終端機，而且不會儲存電子格式持卡人資料的商家

SAQ C-VT
的制定是為了幫助以下商家符合適用規範，這類商家在處理持卡人資料時，僅使用連接網際網路之個人電腦上的隔離虛擬付款終端機。

虛擬終端機是一種藉由網路瀏覽器存取的方式，針對收單機構、處理機構或第三方服務供應商網站而設，其可授權支付卡交易，並讓商戶透過安全連接的網路瀏覽器手動輸入支付卡資料。虛擬終端機與實體終端機的差別在於，其不會直接讀取支付卡資料。支付卡交易是以手動輸入資料的方式來進行。

SAQ C-VT
適用的商家僅透過虛擬終端機處理持卡人資料，不會在任何電腦系統上儲存持卡人資料。這些虛擬終端機透過連接網際網路，以存取託管虛擬終端機支付處理功能之第三方。第三方可以是透過儲存、處理及/或傳輸持卡人資料，來授權及/或結算商家虛擬終端機支付交易的收單機構、處理機構或第三方服務供應商。

本 SAQ 問卷適用的商家，必須透過鍵盤手動輸入單筆交易至網際網路版虛擬終端機解決方案。SAQ C-VT 適用的商家可以是實體 (出示實卡) 或郵購/電話訂購 (無卡支付) 的商家。

SAQ C-VT 適用的商家必須確認其滿足以下針對此支付管道的資格條件：

- 貴公司為完成支付處理，所採用的虛擬終端機，僅透過連接至網際網路的網頁瀏覽器進行存取；
- 貴公司之虛擬終端機解決方案由 PCI DSS 驗證之第三方服務供應商提供並託管；
- 貴公司透過隔離在單獨位置之電腦存取符合 PCI DSS 的虛擬終端機解決方案，此電腦未連接到您環境中其他位置或系統 (可以透過防火牆或網路區段劃分，將此電腦與其他系統隔離開)；
- 貴公司的電腦未安裝可儲存持卡人資料的軟體 (例如，無用於批次處理或儲存與轉寄之軟體)；
- 貴公司的電腦未連接任何用於擷取或儲存持卡人資料的硬體裝置 (例如，未連接連讀卡機)；
- 貴公司未透過任何管道 (例如，透過內部網路或網際網路) 以電子方式接收或傳輸持卡人資料；
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件；**以及**
- 貴公司不儲存電子格式的持卡人資料。

此 SAQ 不適用於電子商務商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ C – 支付應用系統連接到網際網路，而且不儲存電子格式持卡人資料的商家

SAQ C 的制定是為了幫助以下商家符合適用規範，這類商家的支付應用系統 (例如 POS 系統) 連接至網際網路 (例如經由 DSL、纜線數據機等)。

SAQ C 適用的商家透過連接到網際網路的 POS 機，或其它支付應用系統處理持卡人資料，但不會在任何電腦系統上儲存持卡人資料，其可以是實體 (出示實卡) 商家，也可以是電子商務或郵購/電話訂購 (無卡支付) 商家。

SAQ C 適用的商家必須確認其符合以下針對此支付管道的資格條件：

- 貴公司在同一設備及/或區域網路 (LAN) 上既有支付應用系統，又有網際網路連接；
- 支付應用系統/網際網路設備未連接至您環境內任何其它系統 (可以透過網路區段劃分，將支付應用系統/網際網路設備與其他所有系統隔離開來)；
- POS 環境的實體位置未連接到其他營業場所或其他商店位置，而且任何 LAN 僅供單一商店使用；
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件；**以及**
- 貴公司不儲存電子格式的持卡人資料。

此 SAQ 不適用於電子商務商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

SAQ P2PE – 僅使用PCI SSC 清單上 P2PE 解決方案所管理的硬體付款終端機，而且不儲存電子格式持卡人資料的商家

SAQ P2PE 的制定是為了幫助以下商家符合適用規範，這類商家在處理持卡人資料時，僅使用 PCI SSC 清單上所列之經驗證的「點對點加密」(P2PE) 解決方案包含的付款終端機。

SAQ P2PE 適用的商家不會存取任何電腦系統上的純文字帳戶資料，僅會透過 PCI SSC 核准之 P2PE 解決方案中的硬體付款終端機輸入帳戶資料。SAQ P2PE 適用的商家可以是實體 (出示實卡) 或郵購/電話訂購(無卡支付)
商家。例如，如果郵購/電話訂購商家經由紙本或電話接收持卡人資料，然後將其直接輸入經 P2PE 驗證的硬體裝置，則該商家適用 SAQ P2PE。

SAQ P2PE 適用的商家必須確認其符合以下針對此支付管道的資格條件：

- 所有付款處理事宜均透過經 PCI SSC 核准的清單上所列的經驗證的 PCI P2PE 解決方案進行；
- 商家環境中唯一用於儲存、處理或傳輸帳戶資料的系統，是經 PCI 驗證的清單上所列之 P2PE 解決方案的互動點 (POI) 裝置；
- 貴公司不接收或傳輸電子格式的持卡人資料；
- 貴公司的環境內沒有儲存電子格式持卡人資料的舊裝置；
- 貴公司留存的所有持卡人資料均為紙本形式 (如列印的報告或收據)，而且不會透過電子方式接收這些文件；以及
- 貴公司已實施 P2PE 解決方案供應商提供之 *《P2PE 說明手冊》(PIM)* 中的所有管控措施。

此 SAQ 不適用於電子商務商家。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

商家適用的 SAQ D– 其他所有符合 SAQ 資格條件的商家

適用 SAQ D 的商家為所有不包括在前述 SAQ 類型描述中，但具備 SAQ 資格的商家。

適用 SAQ D 之商家環境的範例包括 (但不限於)：

- 網站會接受持卡人資料的電子商務商家；
- 會儲存電子格式持卡人資料的商家；
- 不儲存電子格式持卡人資料，而且不符合其他 SAQ 類型之條件的商家；
- 其環境可能符合另一種 SAQ 類型之條件，但是適用於其他 PCI DSS 要求的商家。

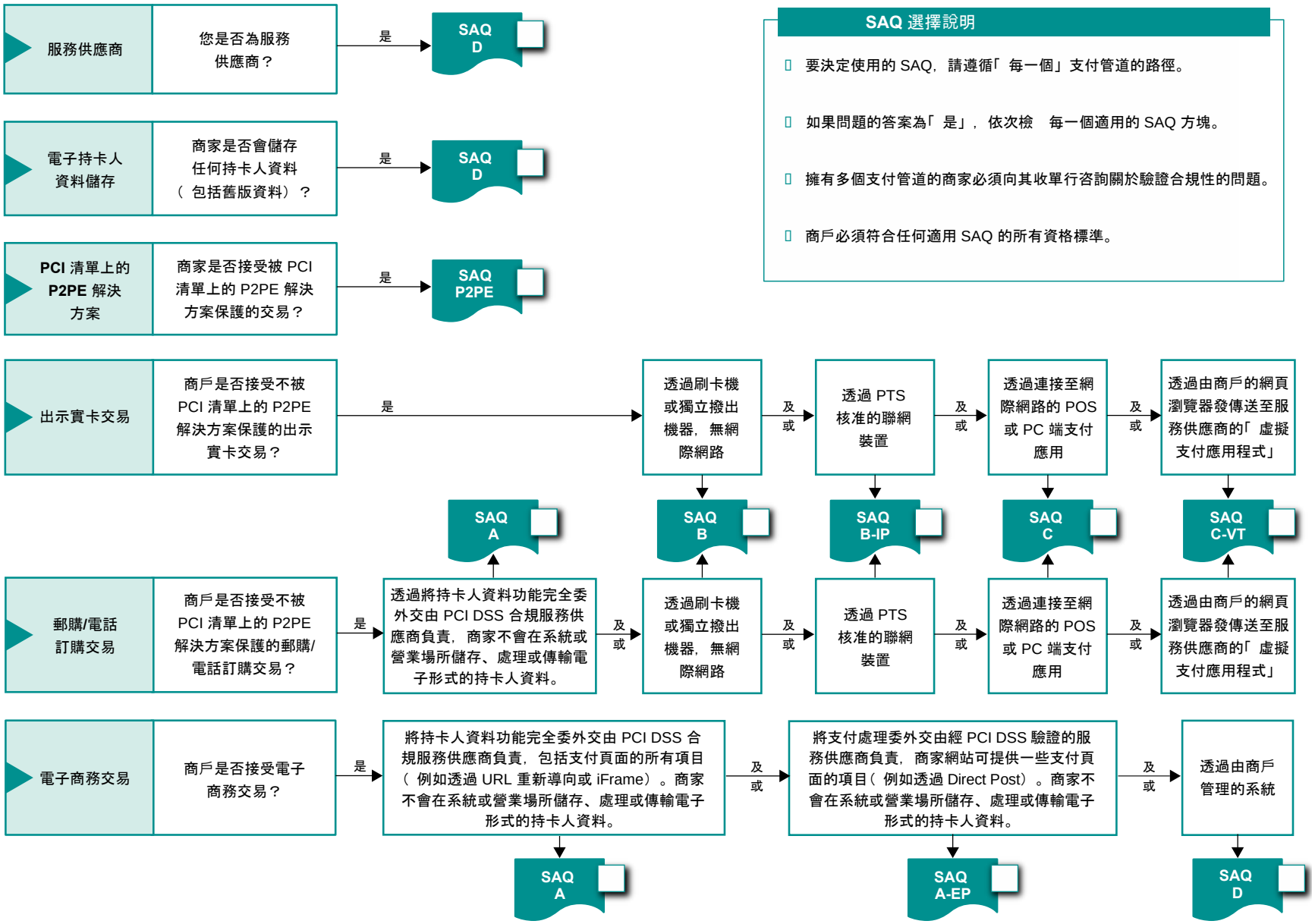
服務供應商適用的 SAQ D– 符合 SAQ 資格條件的服務供應商

適用 SAQ D 的服務供應商為所有由支付品牌定義為符合 SAQ 的資格條件的服務供應商。

附註 (針對商家適用的 SAQ D 與服務供應商適用的 SAQ D)：雖然許多完成 SAQ D 的組織需要驗證是否符合各項 PCI DSS 規範，但是對於一些業務模式非常特殊的組織來說，某些規範可能不適用。例如，如果某公司在任何情況下均不會使用無線技術，則對於 PCI DSS 中針對無線技術管理的部分，該公司不需要驗證其合規性。請參閱下述指南，瞭解有關某些其他特定要求排除事項的資訊。

對於選擇 SAQ 類型的圖表指南，請參閱第 20 頁「哪種 SAQ 最適合我的環境？」

哪種 SAQ 最適合我的環境？



SAQ 選擇說明

- 要決定使用的 SAQ，請遵循「每一個」支付管道的路徑。
- 如果問題的答案為「是」，依次檢　每一個適用的 SAQ 方塊。
- 擁有多個支付管道的商家必須向其收單行咨詢關於驗證合規性的問題。
- 商戶必須符合任何適用 SAQ 的所有資格標準。