支付卡行業 (PCI)
資料安全標準

要求和安全評估程序

2.0 版

2010 年 10 月

文件變更記錄

日期	版本	描述	頁碼
2008 年 10 月	*1.2 版*	*引入 PCI DSS v1.2 作為「PCI DSS 要求和安全評估程序」，消除文件之間的重複，並按照* PCI DSS 安全稽核程序 v1.1 進行了一般和具體變更。*如需完整資訊，請參閱*「PCI 資料安全標準 PCI DSS 1.1 版到 1.2 版變更摘要」。	
2009 年 7 月	*1.2.1 版*	*增加了 PCI DSS v1.1 到 v1.2 被錯誤刪除的句子。*	*5*
		在測試程序 6.3.7.a 和 6.3.7.b 中，將「then」更正為「than」。	*32*
		移除測試程序 6.5.b 內「到位」與「不到位」欄的灰色標記。	*33*
		對於補償性控制工作表 – *完成的範例，將頁面頂部的措辭更改為「對於任何透過補償性控制標注為「到位」的要求，請使用此工作表定義補償性控制」。*	*64*
2010 年 10 月	*2.0 版*	*更新與實施自 v1.2.1 以來的變更。若需詳細資料，請參閱*「PCI DSS - PCI DSS 1.1 版到 1.2 版變更摘要」。	

目錄

引言和 PCI 資料安全標準概要

制定支付卡行業 (PCI) 資料安全標準 (DSS) 以促進並提高持卡人資料安全，有利於全球廣泛採用統一的資料安全標準。PCI DSS 提供用於保護持卡人資料安全的技術與作業要求之基準。PCI DSS 適用於所有涉及支付卡處理之實體，包括商戶、處理機構、購買者、發行商和服務提供商以及儲存、處理或傳輸持卡人資料的所有其他實體。PCI DSS 包括一組保護持卡人資料的基本要求，並可能增加額外的管控措施與實務，以進一步降低風險。以下是 12 條 PCI DSS 要求的高級概要。

PCI 資料安全標準 - 高級概觀

建立並維護安全網路	**1.** 安裝與維護防火牆設定以保護持卡人資料 **2.** 對於系統密碼及其他安全參數，請勿使用供應商提供的預設值
保護持卡人資料	**3.** 保護儲存的持卡人資料 **4.** 加密透過開放的公用網路傳輸的持卡人資料
維護漏洞管理程式	**5.** 使用並定期更新防毒軟體或程式 **6.** 開發並維護安全系統和應用程式
實施嚴格的存取控制措施	**7.** 限制為只有業務需要知道的人才能存取持卡人資料 **8.** 為具有電腦存取權的每個人指定唯一的 ID **9.** 限制對持卡人資料的實際存取
定期監控並測試網路	**10.** 追蹤並監控對網路資源及持卡人資料的所有存取 **11.** 定期測試安全系統和程序。
維護資訊安全政策	**12.** 維護滿足所有人員資訊安全需求的政策。

本文件 (*PCI 資料安全標準要求和安全評估程序*) 將 12 條 PCI DSS 要求與相應的測試程序共同融入到安全評估工具中。本文件用於實體驗證程序的 PCI DSS 合規性評估。以下章節提供詳盡指南和最佳實務，協助實體籌備、執行和報告 PCI DSS 評估結果。「PCI DSS 要求和測試程序」始見於 **第 19 頁。**

PCI 安全標準協會 (PCI SSC) 網站 (www.pcisecuritystandards.org) 包含大量其他資源，其中包括：

- 合規性證明書
- *導覽 PCI DSS：理解資料安全要求的目的*
- *《 PCI DSS 與 PA-DSS 術語、縮寫和首字縮寫》*
- FAQ (常見問題)
- 資訊補充與指南

請參閱 www.pcisecuritystandards.org 瞭解更多內容。

註：*「資訊補充」是 PCI DSS 的補充材料，可確定有助符合 PCI DSS 要求的額外考量因素與建議，但不會變更、消除或取代 PCI DSS 要求或其中任何內容。*

PCI DSS 適用性資訊

只要儲存、處理或傳輸帳戶資料，則 PCI DSS 要求適用。 *帳戶資料*由*持卡人資料*和*敏感驗證資料*構成，如下所示：

持卡人資料包括：	*敏感驗證資料包括：*
▪ 主帳戶 (PAN) ▪ 持卡人姓名 ▪ 到期日期 ▪ 業務代碼	▪ 晶片上的完整磁條資料或與之相當資料 ▪ CAV2/CVC2/CVV2/CID ▪ PIN/PIN 區塊

主帳戶號碼是 PCI DSS 要求適用性的決定性因素。 只要儲存、處理或傳輸主帳戶號碼 (PAN)，則 PCI DSS 要求適用。如果未儲存、處理或傳輸 PAN，則 PCI DSS 與 PA-DSS 不適用。

如果持卡人名稱、服務代碼及/或到期日期透過 PAN 進行儲存、處理或傳輸，或者出現在持卡人資料環境內，則必須按照所有 PCI DSS 要求保護這些資料，但僅適用於 PAN *的*要求 3.3 和 3.4 例外。

PCI DSS
代表一組最起碼的控制目標，這些目標可透過地方、地區與部門的法律法規得以改善。此外，立法或監管要求可能需要具體保護個人身份資訊或其他資料元素
(例如持卡人姓名)，或者定義某個實體有關消費者資訊的披露實務。其範例包括有關消費者資料保護、隱私、身份盜竊或資料安全的立法。PCI DSS 不會取代地方或地區法律、政府法規或其他法律規定。

下表描述了持卡人和敏感驗證資料的常用元素，無論是允許還是禁止每個資料元素的儲存，或者是必須保護每個資料元素。此表並非十分詳盡，但足以說明套用於各個資料元素的不同類型要求。

		資料元素	允許儲存	按照要求 3.4 使儲存的帳戶資料不可讀
帳戶資料	持卡人資料	主帳戶 (PAN)	是	是
		持卡人姓名	是	否
		業務代碼	是	否
		到期日期	是	否
	敏感驗證資料 [1]	完整磁條資料 [2]	否	按照要求 3.2 無法儲存
		CAV2/CVC2/CVV2/CID	否	按照要求 3.2 無法儲存
		PIN/PIN 區塊	否	按照要求 3.2 無法儲存

PCI DSS 要求 3.3 和 3.4 僅適用於 PAN。如果 PAN 與持卡人資料的其他元素一起儲存，則必須按照 PCI DSS 要求 3.4 僅使 PAN 不可讀。

PCI DSS ***僅在***儲存、處理及/或傳輸 PAN 時適用。

1 *敏感驗證資料不得在授權後儲存 (即便是經過加密的)。*

2 *源自磁條的完整追蹤資料，晶片上或其他來源的相當資料。*

PCI DSS 與 PA-DSS 的關係

僅使用符合 PA-DSS 要求之應用程式不足以使實體符合 PCI DSS 要求，因爲此應用程式必須在符合 PCI DSS 要求的環境中依照由支付應用程式供應商編制的《PA-DSS 實施指南》 (按照 PA-DSS 要求 13.1) 實施。

支付應用程式資料安全標準 (PA-DSS) 的要求源自於 *PCI DSS 要求和安全評估程序* (即本文件)。PCI DSS **Error! Hyperlink reference not valid.**詳細說明了支付應用程式必須支援的合規條件，協助客戶達到 PCI-DSS 合規要求。

在符合 PCI DSS 的環境中使用安全支付應用程式，可以將潛在的安全漏洞降至最低，從而防止完整磁條資料、卡驗證碼與驗證值 (CAV2、CID、CVC2、CVV2) 以及 PIN 區塊遭到侵害，並防止因安全漏洞所造成的嚴重欺詐行為。

支付應用程式會有礙於合規性的一些情況包括：

- 授權之後晶片上的磁條資料及/或相當資料被儲存在客戶的網路中；
- 應用程式要求客戶禁用 PCI DSS 所要求的其他功能 (例如殺毒軟體或防火牆)，以便使支付應用程式正常執行；以及
- 供應商使用不安全的方式連接至應用程式，以支援客戶。

PA-DSS
適用於從事支付應用程式開發並將其銷售、發佈或授權給第三方用於儲存、處理或者傳輸持卡人的授權或結算資料的軟體供應商或其他方。

請注意以下有關 PA-DSS 適用性的內容：

- 對於通常以「現貨供應」模式銷售與安裝、無需軟體供應商進行自訂的支付應用程式，***適用*** PA-DSS。
- PA-DSS ***不適用於***由商戶與服務提供商開發的僅在內部使用的支付應用程式 (不銷售、發佈或授權給第三方)，因為此類內部開發的支付應用程式將作為商戶或服務提供商的常規 PCI DSS 合規性審查內容的一部分而被考慮。

若需確定 PA-DSS 是否適用於特定支付應用程式的詳盡指南，請參閱 「PA-DSS 要求和安全評估程序」，此程序可在 www.pcisecuritystandards.org 網站找到。

PCI DSS 要求合規性的評估範疇

PCI DSS 安全要求適用於所有系統元件。PCI DSS 內的「系統元件」定義為包含於持卡人資料環境或與之相關的任何網路元件、伺服器或應用程式。「系統元件」還包括所有虛擬元件，例如虛擬機、虛擬交換機/路由器、虛擬裝置、虛擬應用程式/桌面和 Hypervisor。持卡人資料環境由人員、程序以及儲存、處理或傳輸持卡人資料或敏感驗證資料的技術構成。網路元件包括但不局限於防火牆、交換機、路由器、無線存取點、網路裝置和其他安全裝置。伺服器類型包括但不限於以下類型：Web、應用程式、資料庫、認證、郵件、代理、網路時間協定 (NTP) 和網域名稱伺服器 (DNS)。應用程式包括所有購買和自訂的應用程式，包括內部和外部 (例如網際網路) 應用程式。

PCI DSS 評估的第一步是精確確定審查的範疇。接受評估的實體必須確定持卡人資料的所有位置與流量並確保其包含在 PCI DSS 範疇之內，以確認 PCI DSS 範疇的精確度，此事每年至少要做一次且須在年度評估之前完成。為確認 PCI DSS 範疇的精確度與適當性，須執行以下各項：

- 接受評估的實體確定並記錄環境內存在的所有持卡人資料，以確認沒有持卡人資料位於目前定義之持卡人資料環境 (CDE) 之外。
- 一旦確定並記錄持卡人資料的所有位置，則實體會利用相關結果確認 PCI DSS 範疇是適當的 (例如，結果可能是持卡人資料位址圖表或詳細目錄)。
- 實體可認爲任何被發現的持卡人資料屬於 PCI DSS 評估的範疇之內並且是 CDE 的一部分，除非此類資料被刪除或被遷移/併入當前定義的 CDE。
- 實體保留顯示如何確認 PCI DSS 範疇以及相關結果的文件，以便在下一年度 PCI DSS 範疇確認過程中供評估者審查及/或參考。

網路區段劃分

將持卡人資料環境進行網路區段劃分或與實體網路提醒隔離 (區段劃分) 不是一項 PCI DSS 要求。然而，強烈建議將它作為一種評估方法，以降低：

- PCI DSS 評估的範疇
- PCI DSS 評估的成本
- 實施和維護 PCI DSS 控制的成本和難度
- 機構的風險 (透過將持卡人的資料統一到更少、更易控制的位置來降低風險)

沒有充足的網路區段劃分 (有時稱為「平坦式網路」)，整個網路都處於 PCI DSS 評估範疇中。網路區段劃分可以透過眾多實體或邏輯方法實現，例如正確設定的內部網路防火牆、帶有嚴格存取控制清單的路由器或其他限制存取網路特定區段劃分的技術。

縮小持卡人資料環境範疇的一個前提條件是透徹理解與持卡人資料儲存、處理或傳輸相關的業務需求和過程。透過刪除不必要的資料並集中必要的資料以將持卡人資料限制在盡可能少的位置，這可能需要對長期業務實踐進行重建。

透過資料流圖表記錄持卡人資料流有助於全面瞭解所有的持卡人資料流，並確保任何網路區段劃分在隔離的持卡人資料環境中都有效。

如果網路區段劃分已到位，並且用於縮小 PCI DSS
評估範疇，則評估者必須確認區段劃分足以縮小評估範疇。在高層上，充足的網路區段劃分將儲存、處理或傳輸持卡人資料的系統與那些不進行這些操作的系統隔離開來。然而，網路區段劃分具體實施的充足性非常多變，並且依賴於諸如指定的網路設定、部署的技術以及其他可能實施的控制措施等諸多因素。

*附錄 D：「商業場所/系統元件區段劃分與抽樣」*提供更多有關 PCI DSS 評估範疇之網路區段劃分與抽樣效果的資訊。

無線

如果使用無線技術來儲存、處理或傳輸持卡人資料 (例如，銷售點交易、「快速結賬」)，或者如果無線局域網路 (WLAN)
連接到持卡人資料環境或其部分 (例如，沒有明確使用防火牆隔開)，則無線環境的 PCI DSS 要求和測試程序適用且必須執行 (例如，要求 1.2.3、2.1.1 和 4.1.1)。在實施無線技術之前，實體應該仔細評估抵禦風險的技術需求。僅對非敏感資料傳輸部署無線技術。

第三方/外包

對於要接受年度現場評估的服務提供商，必須對持卡人資料環境內所有系統元件執行合規性驗證。

服務提供商或商戶可能使用第三方提供商代表它們儲存、處理或傳輸持卡人資料，或者管理諸如路由器、防火牆、資料庫、實體安全和/或伺服器等元件。如果是這樣，可能會對持卡人資料環境安全產生影響。

對於那些將持卡人資料的儲存、處理或傳輸外包給第三方服務提供商的實體，合規性報告 (ROC)
必須記錄每家服務提供商的職責，明確接受評估實體適用哪些要求，以及服務提供商適用哪些要求。對於第三方服務提供商，驗證合規性有兩個選項：

1) 他們可以自行執行 PCI DSS 評估並向客戶提供證明其合規性的證據；或者
2) 如果他們沒有自行執行 PCI DSS 評估，則需要在客戶每次執行 PCI DSS 評估期間審查自己的服務。

請參閱以下「合規性報告的說明和內容」章節中第 3 項「審查環境詳細資料」之「有關管理服務提供商 (MSP) 審查」瞭解更多內容。

此外，商戶和服務提供商必須管理並監管所有能夠存取持卡人資料的相關第三方服務提供商的 PCI DSS 合規性。*請參閱本文件中的「要求 12.8」以瞭解詳細資料。*

業務場所/系統元件抽樣

抽樣並非一項 PCI DSS 要求。然而，在考量受評估環境之整體範疇與複雜性之後，評估者可獨立選擇商業場所/系統元件之代表性樣本，以評估 PCI DSS

要求。這些樣本必須首先依據商業場所定義，然後依據每個選定商業場所內的系統元件定義。樣本必須是從商業場所的所有類型與位置以及選定商業場所內系統元件類型中選擇出的代表性樣本。樣本必須足夠大，如此方可向評估者確保控制措施能按照預期實施。

為評估所做的商業場所/系統元件抽樣不會縮小持卡人資料環境的範疇或者降低 PCI DSS 要求的適用性。無論是否使用抽樣，PCI DSS 要求都適用於整個持卡人資料環境。如果使用抽樣，則每個樣本必須依照所有適用之 PCI DSS 要求進行評估。不允許對 PCI DSS 要求實施抽樣。

商業場所範例包括但不限於：公司辦公室、商店、特許經銷場所、資料中心以及不同位置的其他場所類型。抽樣應該應包含每個選定業務場所的系統元件。例如，對於每個選定之業務場所，包含適用於受評估區域的各種作業系統、功能和應用程式。

舉例而言，評估者可以定義一個商業場所的樣本包含執行 Apache WWW 的 Sun 伺服器、執行 Oracle 的 Windows 伺服器、執行舊有的卡處理應用程式的主機系統、執行 HP-UX 的資料傳輸伺服器，以及執行 MYSQL 的 Linux 伺服器。如果所有應用程式都在單一版本的作業系統 (例如 Windows 7 或 Solaris 10) 上執行，則抽樣仍應包含多個應用程式 (例如資料庫伺服器、Web 伺服器、資料傳輸伺服器)。

在獨立選擇業務場所/系統元件抽樣時，評估者應考慮以下方面：

- 如果存在可確保一致性且每個商業場所/系統元件必須遵循的標準而集中的 PCI DSS 安全和作業程序與到位的管控措施，樣本必須小於標準程序/到位的管控措施不存在的情況。樣本必須大到足以向評估者充分保證所有的商業場所/系統元件均是依照標準程序設定。
- 如果存在超過一個類型之標準安全及/或到位的作業程序 (例如，抽樣包括不同類型之商業場所/系統元件)，則樣本必須大到每類程序均足以包含安全的商業場所/系統元件。
- 如果不存在標準 PCI DSS 程序/到位的管控措施，且每個商業場所/系統元件是透過非標準程序管理的，則樣本必須更大，這樣才能向評估者保證每個商業場所/系統元件均已適當實施 PCI DSS 要求。

對於使用抽樣方法的每個範例，評估者必須：

- 記錄抽樣技術與樣本大小之後的邏輯依據，
- 記錄並驗證所使用之標準 PCI DSS 程序與管控措施，以確定樣本大小，以及
- 解釋樣本對於整個目標人群的適當性與代表性。

另請參閱：
附錄D：商業場所/系統元件區段劃分與抽樣。

評估者必須重新驗證每次評估抽樣的邏輯依據。如果使用抽樣方法，則每次評估必須使用不同的商業場所和系統元件樣本。

補償性控制

補償性控制每年都必須由評估者記錄、檢查和驗證，並與合規性報告一起提交，其根據是*附錄 B：補償性控制*和*附錄 C：補償性控制工作表*。

對於每項和每次補償性控制，補償性控制工作表 *(附錄 C)* **必須** 完成。此外，補償性控制結果必須記錄在相應 PCI DSS 要求部分的 ROC 中。

參見上述 *附錄B* 和 *C* 以瞭解關於「補償性控制」的詳細資料。

合規性報告的說明與內容

此文件必須用作編制*合規性報告*的範本。被評估的機構應該遵守每個支付品牌相應的報告要求，以確保每個支付品牌知悉機構的合規性狀態。聯絡每個支付品牌以確定報告要求和說明。

報告內容和格式

在完成合規性報告時請遵守這些報告內容和格式的說明：

1. **報告摘要**

   包括以下內容：

   - 描述機構的支付卡業務，包括：
     - 它們在支付卡中的業務角色，也就是它們如何以及為何儲存、處理和/或傳輸持卡人資料

       註： *這不應該是從機構網站上複製和粘貼的內容，而應該是有針對性的描述，使評估者能夠理解支付和機構的角色。*
     - 它們如何處理支付 (直接、間接等)
     - 它們提供什麼類型的支付管道，例如離卡 (如郵件訂購-電話訂購 (MOTO)、電子商務)或持卡
     - 任何連接進行支付傳輸或處理 (包括處理商關係)的機構
   - 機構網路拓樸的高級網路圖表 (從機構獲得或由評估者建立)，包括：
     - 進出網路的連接
     - 持卡人資料環境內的關鍵元件，包括 POS 裝置、系統、資料庫和 Web 伺服器 (視情況而定)
     - 其他需要的支付元件 (視情況而定)

2. 工作範疇和採用方法的描述

根據本文件中的評估範疇部分描述範疇，包括以下方面：

- 記錄評估者如何驗證評估的 PCI DSS 範疇的精確度，包括：
  - 用於確定並記錄持卡人資料所有存在的方法或程序
  - 如何評估與記錄結果
  - 如何確認所使用之方法的有效性與精確度
  - 評估者驗證評估的範疇是精確且適當的。
- 評估集中的環境 (例如，用戶端 Internet 存取點、內部公司網路、處理連接等)
- 如果採用了網路區段劃分，並且用於縮小 PCI DSS 檢查範疇，則只需簡單說明區段劃分以及評估者如何驗證區段劃分的有效性
- 如果評估時使用抽樣方法，則對於每個所選樣本組 (商業場所/系統元件)，須記錄以下內容：
  - 總人數
  - 抽樣數量
  - 選擇抽樣的基本原理
  - 描述如何使用標準的 PCI DSS 安全和作業程序來確定樣本大小以及如何驗證程序/管控措施
  - 樣本對於整個目標人群的適當性與代表性
  - 說明排除在審查範疇以外的儲存、處理或傳輸持卡人資料的任何位置或環境，以及這些位置/環境為什麼被排除在外
- 列舉所有要求遵守 PCI DSS 的全資機構，以及它們是否被單獨檢查或作為此評估的部分接受檢查
- 列舉所有要求遵守 PCI DSS 的國際實體，以及它們是否被單獨審查或作為此評估的部分接受審查
- 列舉所有連接或可能影響持卡人資料環境的無線 LAN 和/或無線支付應用程式 (例如 POS 終端)，並且說明這些無線環境的安全性
- 實施評估使用的 PCI DSS 要求和安全評估程序文件的版本

3. 審查環境的詳細資料

本章節包含以下詳細資料：

- 每條通訊連結的圖表 (包括 LAN、WAN 或 Internet)
- 持卡人資料環境的說明，例如：
  - 持卡人資料的文檔傳輸和處理，包括認證、留存、結算、收費和其他適用的流程
  - 儲存持卡人資料的檔案和表格清單，由評估者建立
    (或從客戶處獲取)並保留在工作文書中的清單提供。此清單應該包括每個持卡人的資料儲存 (檔案、表格等)：
    - 儲存持卡人資料的所有元素的清單
    - 如何保護資料
    - 如何記錄對資料儲存的存取
- 持卡人資料環境中使用的硬體和主要軟體清單，並附帶其各自的功能/用法說明
- 與實體共用持卡人資料之服務提供商及其他第三方的清單

  註： *這些實體必須遵循 PCI DSS 要求 12.8。)*
- 正在使用的第三方支付應用程式產品和版本號清單，包括每個支付應用程式是否已按照 PA-DSS 驗證過。即使支付應用程式已經 PA-DSS 驗證過，評估者仍需要驗證應用程式已按符合 PCI DSS 要求的方式和環境實施，並且遵守支付應用程式供應商的 *PA-DSS 實施指南*。

  註： *這不是使用 PA-DSS 驗證應用程式的一項 PCI DSS 要求。請分別諮詢每個支付品牌以瞭解它們的 PA-DSS 合規要求。)*
- 接受訪問之個人及其組織、職務和訪問主題清單
- 審查的文件清單
- 對於管理服務提供商 (MSP) 檢查，評估者必須明確指出本文件中的哪些要求適用於 MSP (並且包含在審查中)和哪些不包含在審查中，以及哪些是 MSP 客戶的責任，應包含在它們的審查中。包含的資訊涉及哪些 MSP IP 位址作為 MSP 季度漏洞掃描的部分進行掃描，以及哪些 IP 位址是 MSP 客戶的責任，應包含在它們自己的季度掃描中。

4. 聯絡資訊與報告日期

包括：

- 商戶或服務提供商和評估者的聯絡資訊
- 評估的時間範疇 — 指定評估的持續時間和時間間隔
- 報告日期

5. 季度掃描結果

- 報告摘要和要求 11.2.2 註解中總結最近 4 個季度的 ASV 掃描結果。

> ***註：*** *如果評估者確認以下各項，則對於初始 PCI DSS 合規性評估，不要求完成最近四個季度的掃描：*
>
> *1) 最近的掃描結果成功通過，*
>
> *2) 實體已經記錄要求繼續執行季度掃描的政策和程序，以及*
>
> *3) 初始掃描中指出的漏洞在重新掃描時顯示已更正。*
>
> *第一次 PCI DSS 審查完成之後的年度中，必須通過了四次季度掃描。*

- 掃描必須根據 *「PCI 認可掃描供應商 (ASV) 程式指南」覆蓋實體中所有外部可存取 (面向 Internet) 的 IP 位址。*

6. 結果與觀察結論

在實施摘要中總結任何可能與標準合規性範本格式不符的結果。

所有評估者 *必須：*

- 使用詳細的 PCI DSS 要求和安全評估程序範本來提供關於每項要求和子要求的詳細報告說明和結果。
- 確保清楚地解釋所有 N/A 回應。
- 審查並記錄考慮到的任何補償性控制，以確認控制是到位的。

*請參閱*以上「補償性控制」章節和*附錄 B* 及 *C*，以獲得關於補償性控制的更多資訊。

未清項目的再驗證

要求「採用控制」報告來驗證合規性。如果此報告含有「未清項目」或者在將來日期完成的項目，則被認為是非合規報告。商戶/服務提供商必須在認證完成以前解決這些項目。在商戶/服務提供商解決這些未清項目以後，評估者將重新評估以驗證糾正措施已採用和所有要求均已達到。重新驗證以後，評估商將發佈新的合規性報告，確認持卡人資料環境完全合規，並且按照說明進行提交 (請參閱下文)。

PCI DSS 合規 – 完成步驟

1. 根據以上標題為「合規性報告的說明與內容」章節完成合規性報告 (ROC)。
2. 確保通過漏洞掃描已由 PCI SSC 認證的掃描供應商 (ROC) 完成，並從 ASV 獲得通過掃描證明。

3. 視情況全部完成服務提供商或商戶的合規性證明。合規性證明見於 PCI SSC 網站 (www.pcisecuritystandards.org)。
4. 向購買者 (對於商戶)支付品牌或其他請求者 (對於服務提供商)提交 ROC、通過掃描的證明、合規性證明和其他要求的文件。

詳細的 PCI DSS 要求和安全評估程序

對於 *PCI DSS 要求和安全評估程序*，定義表格欄標題的內容如下：

- **PCI DSS 要求** - 此欄定義了資料安全標準並列示了要求，以實現 PCI DSS 合規性；合規性必須按照這些要求進行驗證。
- **測試程序** - 此欄表明評估者遵從的程序，以驗證 PCI DSS 要求是「到位」的。
- **到位** — 評估者必須使用此欄簡短描述對於每項要求已驗證為「到位」的那些管控措施，包括描述由補償性控制或「未到位」之要求造成的管控措施。
- **未到位** - 評估者必須使用此欄來提供那些未到位管控措施的簡短描述。請注意，非合規報告不應該提交給支付品牌或購買者，除非特別要求。，若需非合規報告的詳細說明，請訪問 PCI SSC 網站 (www.pcisecuritystandards.org)，參閱「合規性證明」。
- **目標日期/註解 -**
  對於那些「未到位」的管控措施，評估者可以納入商家或服務提供商預計控制「到位」的目標日期。任何額外的備註或註解也可納入其中。

註：
對於仍未到位的項目或尚未完成的未清項目，一定不能使用此欄。

建立並維護安全網路

要求 1：　　安裝並維護防火牆設定，以保護持卡人資料

防火牆是控制實體網路 (內部) 和未信任網路 (外部)
之間的電腦流量，以及控制進出實體內部受信任網路之更敏感區域流量的裝置。持卡人資料環境是實體受信任網路內部更敏感區域的一個範例。

防火牆負責檢查所有網路流量，並阻止那些不符合特定安全標準的傳輸活動。

所有系統必須受到保護，防止從不受信任網路進行未授權存取，無論是透過 Internet 以電子商務形式、員工透過桌面瀏覽器進行的 Internet 存取、員工電子郵件存取、諸如企業對企業連接的專門連接、透過無線網路或是其他途徑進入系統。通常看似無關緊要進出不受信任網路的途徑都可能成為關鍵系統的未保護入口。防火牆是所有電腦網路的關鍵保護機制。

如果達到要求 1
規定之防火牆的最起碼要求，則其他系統元件可以提供防火牆功能。如果在持卡人資料環境內使用其他系統元件提供防火牆功能，則這些裝置必須納入要求 1 的範疇與評估內容之中。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
1.1 建立包含以下各項的防火牆和路由器設定標準：	**1.1** 獲取並檢查以下防火牆和路由器設定標準及下文指定的其他文件，以驗證標準是完整的。完成以下各項：			
1.1.1 批准和測試所有網路連接以及防火牆和路由器設定變更的正式程序	**1.1.1** 確認具有批准和測試所有網路連接以及防火牆和路由器設定變更的正式程序。			
1.1.2 具有包含持卡人資料所有連接的最新網路圖 (包括所有無線網路)	**1.1.2.a**確認具有最新網路圖 (例如，一個表明網路中持卡人資料程序的圖表)，並且它記錄了至持卡人資料的所有連接，包括所有無線網路。			
	1.1.2.b 確認圖表是最新的。			
1.1.3 要求在每個網際網路連接以及在任何非軍事區域 (DMZ) 和內部網路區域之間建立防火牆	**1.1.3.a** 確認防火牆設定標準包括在每個網際網路連接以及任何 DMZ 與內部網路區域之間建立防火牆的要求。			
	1.1.3.b 確認最新網路圖與防火牆設定標準一致。			
1.1.4 描述網路元件邏輯管理的群組、角色和責任	**1.1.4**確認防火牆和路由器設定標準包括關於網路元件邏輯管理的群組、角色和責任的描述。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
1.1.5 針對所有允許使用的服務、通訊協定和連接埠的使用提供相關文件和商業論證，包括為被視為不安全的通訊協定實施安全功能的文件。 非安全服務、通訊協定和連接埠的範例包括但不限於 FTP、Telnet、POP3、IMAP 和 SNMP。	**1.1.5.a** 確認防火牆和路由器設定標準包括一個業務需要的服務、通訊協定和連接埠 (例如，超文字傳輸協定 (HTTP) 和安全通訊端層 (SSL)、安全殼層 (SSH) 和虛擬專用網路 (VPN) 協定)的文件清單。			
	1.1.5.b 識別允許的不安全服務、通訊協定和連接埠；並且確認它們是必需的，而且每項服務的安全功能已按檢測防火牆和路由器設定標準進行了記錄和實施。			
1.1.6 要求至少每六個月對防火牆和路由器規則集進行一次審查	**1.1.6.a確認防火牆和路由器設定標準要求至少每 6 個月審查一次防火牆和路由器規則設定集。**			
	1.1.6.b獲取並檢查確認至少每 6 個月審查一次規則設定集的文件。			
1.2 設定一個限制持卡人資料環境中不受信任網路和任何系統元件之間的防火牆和路由器設定。 ***註：*** *「不受信任的網路」是指在接受審查的實體網路之外的任何網路，和/或實體無法控制或管理的任何網路。*	**1.2**檢查防火牆和路由器設定，以確認持卡人資料環境中不受信任網路和系統元件之間的連接受到限制，如下所示：			
1.2.1 根據持卡人資料環境的需要限制輸入和輸出流量。	**1.2.1.a** 確認進出流量受到持卡人資料環境需要的限制，並且對這些限制進行了記錄。			
	1.2.1.b確認其他所有進出流量都是明確禁止的，例如透過使用明示的「禁止所有」或允許聲明後的暗示禁止。			
1.2.2 保護並同步處理路由器設定檔案。	**1.2.2** 確認路由器設定檔案是安全且同步的，例如執行設定檔案 (用於正常的路由器執行)和啟動設定檔案 (當機器重新啟動時使用)有相同的安全設定。			
1.2.3 在任何無線網路和持卡人資料環境之間安裝週邊防火牆，並且將這些防火牆設定為禁止或控制 (如果出於業務目的需要這樣的流量)從無線環境流入持卡人資料環境的任何流量	**1.2.3** 確認在任何無線網路和儲存持卡人資料的系統之間安裝了週邊防火牆，並且這些防火牆禁止或控制 (如果出於業務目的需要這樣的流量)從無線環境流入持卡人資料環境的任何流量。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
。				
1.3禁止在持卡人資料環境中的 Internet 和任何系統元件之間的直接公共存取。	**1.3** 檢查防火牆和路由器設定 — 包括但不限於網際網路的扼流路由器、DMZ 路由器與防火牆、DMZ 持卡人區段、週邊路由器以及內部持卡人網路區段 — 用於確定網際網路與內部持卡人網路區段內系統元件之間不存在直接存取的情況，如下所示。			
1.3.1 實施 DMZ，使輸入流量僅流入可提供經授權公共存取服務、通訊協定和連接埠的系統元件。	**1.3.1** 確認已實施 DMZ 使輸入流量僅流入可提供經授權的公共存取服務、通訊協定和連接埠的系統元件。			
1.3.2 限制進入 DMZ 內部 IP 位址的 Internet 輸入流量。	**1.3.2** 確認進入 DMZ 內部 IP 位址的 Internet 輸入流量受到限制。			
1.3.3 不允許 Internet 和持卡人資料環境之間進出流量透過直接連接實現。	**1.3.3** 確認不允許 Internet 和持卡人資料環境之間進出流量透過直接連接實現。			
1.3.4 不允許從 Internet 至 DMZ 的內部位址通過。	**1.3.4確認從 Internet 至 DMZ 的內部位址不能通過。**			
1.3.5 不允許未經授權的輸出流量從持卡人資料環境進入 Internet。	**1.3.5** 確認從持卡人資料環境至 Internet 的輸出流量得到明確授權			
1.3.6 實施狀態檢測，亦稱為動態封包過濾。(也就是只有「建立」的連接才允許進入網路。)	**1.3.6** 確認防火牆執行狀態檢測 (動態封包過濾)。(僅建立的連接並當它們與以前建立的工作階段存在關聯時，方允許進入。)			
1.3.7 妥善放置儲存持卡人資料 (例如資料庫) 的系統元件到內部網路區域內，並且與 DMZ 和其他不受信任的網路隔離開來。	**1.3.7** 確認儲存持卡人資料的系統元件位於內部網路區域，並且與 DMZ 和其他不受信任的網路隔離開來。			
1.3.8 切勿向未經授權的各方洩露專用 IP 位址和路由資訊。 ***註：*** *掩蓋 IP 位址的方法包括但不限於：* ▪ *網路位址轉換 (NAT)*	**1.3.8.a** 確認方法到位，以防止專用 IP 位址和路由資訊從內部網路洩漏至 Internet。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
▪ *將包含持卡人資料的伺服器放置到代理伺服器/防火墻或內容快取區之後，* ▪ *移除或過濾那些使用註冊位址的專用網路的路由廣告，* ▪ *內部使用 RFC1918 位址空間，而不是註冊位址。*	**1.3.8.b** 確認任何洩漏專用 IP 位址和路由資訊至外部實體的行爲得到授權。			
1.4 在直接連接至 Internet 的任何行動和/或員工自有電腦上 (例如員工使用的筆記型電腦) 安裝個人防火牆軟體，用於存取組織網路。	**1.4.a** 確認在直接連接至 Internet 的行動和/或員工自有並用於存取組織網路的電腦上 (例如員工使用的筆記型電腦) 安裝並啟動了個人防火牆軟體。			
	1.4.b 確認組織將個人防火牆軟體設定為特定的標準，並且行動和/或員工自有電腦使用者無法對其變更。			

要求 2：　　對於系統密碼及其他安全參數，請勿使用供應商提供的預設值

惡意個人 (實體外部和內部)
通常使用供應商預設密碼和其他供應商預設設定來危害系統。這些密碼和設定為駭客社群所熟知，並且容易透過公開資訊判斷得出。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
2.1 在網路上安裝系統**之前**，務必變更供應商提供的預設設定，包括但不限於密碼、簡單網路管理協定 (SNMP) 社群字串，並刪除不必要的帳戶。	**2.1** 選擇一個系統元件樣本，並嘗試使用供應商提供的預設帳戶和密碼登入到 (在系統管理員的幫助下)裝置，以確認預設帳戶和密碼已變更。 (使用供應商手冊和 Internet 上的資源來查找供應商提供的帳戶/密碼。)			
2.1.1 對於連接到持卡人資料環境或傳輸持卡人資料的無線環境，**變更無線供應商預設設定，包括但不限於預設無線加密金鑰、密碼和 SNMP 社群字串。**	**2.1.1** 確認以下有關供應商對無綫環境之預設設定的各項內容：			
	2.1.1.a 加密金鑰已在安裝時變更了預設值，並且在任何知道金鑰之人離開公司或改變崗位後隨時變更			
	2.1.1.b 確認無線裝置上的預設 SNMP 社群字串已變更。			
	2.1.1.c 確認存取點上的預設密碼/複雜密碼已變更。			
	2.1.1.d 確認無線裝置上的韌體已升級，可支援對無線網路上的驗證和傳輸強效加密。			
	2.1.1.e 確認其他與安全相關的無綫供應商的預設設定已變更 (若適用)。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
2.2 制定所有系統元件的設定標準。確保這些標準解決了所有已知的安全漏洞，並且符合行業接受的系統安全標準。 行業認可系統強化標準的來源包括但不限於： ▪ 網際網路安全中心 (CIS) ▪ 國際標準組織 (ISO) ▪ 系統管理員稽核網路安全 (SANS) 研究所 ▪ 美國國家標準技術研究所 (NIST)	**2.2.a** 檢查組織為所有類型系統元件制定的系統設定標準，並確認系統設定標準與行業認可的強化標準一致。			
	2.2.b 確認按照要求 6.2 在發現新漏洞問題時更新系統設定標準。			
	2.2.c 確認在設定新系統時套用了系統設定標準。			
	2.2.d 確認系統設定標準包含以下各項 (2.2.1 – 2.2.4)。			
2.2.1 每台伺服器僅實施一項主要功能，以防止要求不同安全層級的功能在相同伺服器上共存。 (例如，Web 伺服器、資料庫伺服器和 DNS 應該在獨立的伺服器上實施。) ***註：*** *如果使用虛擬技術，則每個虛擬系統元件僅實施一項主要功能。*	**2.2.1.a** 對於系統元件樣本，確認每台伺服器只執行一項主要功能。			
	2.2.1.b 如果使用虛擬技術，則確認每個虛擬系統元件或裝置僅實施一項主要功能。			
2.2.2 僅啓用系統功能需要的必需且安全的服務、通訊協定和守護程序等。 對任何被視爲不安全的必要服務、通訊協定或守護程序實施安全功能 — 例如，使用諸如 SSH、S-FTP、SSL 或 IPSec VPN 等安全技術，保護諸如 NetBIOS、檔案共用、Telnet、FTP 等不安全的服務。	**2.2.2.a** 對於系統元件樣本，檢測啟用的系統服務、守護程序和通訊協定。確認僅啓用必要的服務或通訊協定。			
	2.2.2.b 確定任何啓用的不安全的服務、守護程序和通訊協定。確認它們均得到驗證，並且安全功能得到記錄與實施。			
2.2.3 設定系統安全參數，防止濫用。	**2.2.3.a**訪問系統管理員和/或安全經理，以確認他們知道系統元件的一般安全參數設定。			
	2.2.3.b確認一般安全參數設定包含在系統設定標準中。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
	2.2.3.c 對於系統元件樣本，確認一般安全參數進行了正確的設定。			
2.2.4 移除所有不必要的功能，例如指令碼、驅動程式、功能、子系統、檔案系統和不必要的 Web 伺服器。	**2.2.4.a** 對於系統元件樣本，確認所有不必要的功能 (例如指令碼、驅動程式、功能、子系統、檔案系統等) 都已移除。			
	2.2.4.b. 確認啓用的功能得到妥善記錄並可支援安全設定。			
	2.2.4.c. 確認僅有記錄的功能呈現在抽樣的系統元件上。			
2.3 使用強效加密對所有非主控台管理的存取進行加密。對於基於 Web 的管理和其他非控制台管理的存取使用諸如 SSH、VPN 或 SSL/TLS 等技術。	**2.3** 對於系統元件樣本，確認非控制台管理的存取已透過下列方式加密：			
	2.3.a 觀察管理員登入到每個系統，以確認在要求提供管理員密碼之前啓用了強效加密方法。			
	2.3.b 審查系統上的服務和參數檔案，以確定 Telnet 和其他遠端登入指令不能內部使用。			
	2.3.c 確認管理員對基於 Web 管理介面的存取是經過強效加密法加密的。			
2.4 共用託管提供商必須保護每個實體託管的環境和持卡人資料。這些提供商必須滿足*「附錄 A：針對共用託管提供商的額外 PCI DSS 要求」中詳細規定的具體要求。*	2.4**執行測試程序 A.1.1** 至 **A.1.4**，詳見 *「附錄 A：針對共用託管提供商的額外 PCI DSS 要求」*)以進行共用託管提供商的 PCI DSS 評估，確認共用託管提供商保護了它們實體 (商戶和服務提供商)的托管環境和資料。			

保護持卡人資料

要求 3：　　保護儲存的持卡人資料

保護方法(例如加密、截斷、遮罩和雜湊等)是持卡人資料保護的關鍵元件。如果入侵者規避了其他網路安全管控措施並存取了加密資料，如果沒有正確的加密金鑰，則其仍無法讀取並使用這些資料。其他保護儲存資料的有效方法應視為可能會降低風險的措施。例如，最小化風險的方法包括：除非絕對必要否則不儲存持卡人資料，不需要完整的 PAN
時截斷持卡人資料，以及不使用諸如電子郵件和即時通訊等最終使用者通訊技術傳送未受保護的 PAN。

請參閱*《PCI DSS 與 PA-DSS 術語、縮寫和首字縮寫》*，瞭解「強效密碼編譯」和其他 PCI DSS 詞彙。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
3.1 實施資料保留和處理政策和程序，最低程度地儲存持卡人資料，如下所示。	**3.1獲取並檢查資料保留和處理政策和程序，並執行以下項目：**			
3.1.1 實施包括如下內容的資料保留和處理政策： ▪ 依照法律、法規和業務要求限制資料儲存數量和保留時間 ▪ 用於安全刪除不再需要之資料的程序 ▪ 持卡人資料的具體保留要求 ▪ 使用季度自動或手動程序，確定並安全刪除已儲存但超出定義之保留要求的持卡人資料	**3.1.1.a** 確認政策和程序已實施，並包含資料保留的法律、法規和業務要求，包括持卡人資料保留的具體要求 (例如，持卡人資料因 Y 業務原因需要保留 X 時長)。			
	3.1.1.b 確認政策和程序包含因法律、法規或業務原因不再需要之資料安全處理的規定，包括持卡人資料處理。			
	3.1.1.c 確認政策和程序涵蓋所有儲存的持卡人資料。			
	3.1.1.d 確認政策和程序至少包括以下一項內容： 程式化程序 (自動或手動)，用於移除已儲存但超出資料保留政策定義之要求的持卡人資料 (至少每季度實施一次) 審查要求 (至少每季度實施一次)，用於確認儲存的持卡人資料沒有超出資料保留政策定義之要求。			
	3.1.1.e 對於儲存持卡人資料的系統元件樣本，確認儲存的資料沒有超出資料保留政策定義之要求。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
3.2 切勿在授權後儲存敏感的驗證資料 (即使已經加密)。 敏感驗證資料包括下文要求 3.2.1 至 3.2.3 中列舉的資料： ***註：*** *如果存在正當業務理由且資料得到安全儲存，則發行商和公司可支援發行服務，以儲存敏感驗證資料。*	**3.2.a** 對於支援發行服務並儲存敏感驗證資料的發行商及/或公司，確認存在儲存敏感驗證資料的正當業務理由，並且資料得到安全儲存。			
	3.2.b 對於所有其他實體，如果接收和刪除了敏感驗證資料，須獲取並審查安全刪除資料的程序，確認資料無法恢復。			
	3.2.c 對於以下敏感認證資料的各項執行以下步驟：			
3.2.1 切勿儲存磁條任意磁軌上的完整內容 (位於卡背面的磁條上，晶片上或其他位置包含的相當資料)。此類資料也可稱為完整磁軌、磁軌、磁軌 1、磁軌 2 及磁條資料。 ***註：*** *在正常的業務過程中，可能需要保留以下磁條資料元素：* ▪ *持卡人的姓名* ▪ *主帳戶 (PAN)* ▪ *到期日期* ▪ *業務代碼* *為將風險降至最低，只儲存業務所需的資料元素。*	**3.2.1** 對於系統元件樣本，檢查包括但不限於以下各項的資料來源，並確認卡背面磁條的任何磁軌上的全部內容或晶片上的相當資料均未在任何環境下儲存： ▪ 輸入的交易資料 ▪ 所有日誌 (例如交易、歷史、偵錯、錯誤) ▪ 歷史檔案 ▪ 跟蹤檔案 ▪ 幾種資料庫模式 ▪ 資料庫內容			
3.2.2 切勿儲存用於驗證離卡交易的卡驗證代碼或值 (印在支付卡正面或背面的三或四位數字)。	**3.2.2** 對於系統元件樣本，檢查包括但不限於以下各項的資料來源，並確認印在卡正面或簽名欄上的三位或四位數的卡驗證代碼或值 (CVV2、CVC2、CID、CAV2 資料) 沒有在任何情況下儲存： ▪ 輸入的交易資料 ▪ 所有日誌 (例如交易、歷史、偵錯、錯誤) ▪ 歷史檔案 ▪ 跟蹤檔案 ▪ 幾種資料庫模式 ▪ 資料庫內容			
3.2.3 切勿儲存個人識別碼 (PIN)	**3.2.3**			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
或加密的 PIN 區塊。	對於系統元件樣本，檢查包括但不限於以下各項的資料來源，並確認 PIN 和加密的 PIN 區塊沒有在任何情況下儲存： ▪ 輸入的交易資料 ▪ 所有日誌 (例如交易、歷史、偵錯、錯誤) ▪ 歷史檔案 ▪ 跟蹤檔案 ▪ 幾種資料庫模式 ▪ 資料庫內容			
3.3 顯示 PAN 時對其進行適當掩蓋 (最多可顯示前六位與後四位數字)。 ***註：*** ▪ *此要求不適用於那些因合法業務需要查看完整的 PAN 的員工和其他方。* ▪ *如果針對銷售點 (POS) 收據等持卡人資料顯示有更加嚴格的要求，則本要求不會取代此類要求。*	**3.3** 獲取並檢查書面政策，檢查 PAN 顯示 (例如螢幕、紙本收據)，以確認在顯示持卡人資料時主帳戶 (PAN) 被掩蓋，除非因合法業務需要而查看完整的 PAN。			
3.4 使用以下任何方法使得任何地方儲存的 PAN 不可讀 (包括在可攜帶數位媒體、備份媒體、日誌中)： ▪ 基於強效密碼編譯的單向雜湊 (雜湊必須應用於整個 PAN) ▪ 截斷 (雜湊不得用於取代 PAN 被截斷的區段) ▪ 索引 Token 與 Pad (必須安全地儲存 Pad) ▪ 帶有相關金鑰管理程序和過程的強效加密法 ***註：*** *如果可以存取 PAN 的截斷與雜湊版本，惡意之人可以相對輕鬆地重建原始 PAN 資料。凡同一 PAN 的雜湊與截斷版本呈現在實體環境內，必須採取額外的管控措施以確保雜湊與截斷版本不會被用於重建原始 PAN。*	**3.4.a** 獲取並檢查用於保護 PAN 之系統的文件，包括供應商、系統/程序類型以及加密演算法 (視情況而定)。確認使用以下任一方法使 PAN 實現不可讀性： ▪ 基於強效密碼編譯的單向雜湊 ▪ 截斷 ▪ 索引記號與索引簿，索引簿必須安全地儲存 ▪ 帶有相關金鑰管理程序和過程的強效加密法			
	3.4.b 檢查資料存放樣本中的多個表格或檔案，以確認 PAN 被設為不可讀 (也就是不以純文字儲存)。			
	3.4.c 檢查卸除式媒體的樣本 (例如備份磁帶)，以確認 PAN 被設為不可讀。			
	3.4.d 檢查稽核日誌樣本，以確認 PAN 已設為不可讀或從日誌中移除。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
3.4.1 如使用了磁碟加密 (而不是檔案級或欄級資料庫加密)，則對邏輯存取的管理必須獨立於本地作業系統的存取控制機制 (例如，不使用本機使用者帳戶資料庫)。解密金鑰決不能與使用者帳戶綁定。	**3.4.1.a** 如果使用了磁碟加密，確認透過獨立於本機作業系統機制的機制(例如，不使用本機使用者帳戶資料庫)執行了對加密檔案系統的邏輯存取。			
	3.4.1.b確認加密金鑰被安全儲存 (例如，儲存在透過嚴格存取控制進行充分保護的卸除式媒體上)。			
	3.4.1.c 確認卸除式媒體上的持卡人資料在進行任儲存時都進行了加密。 ***註：*** *如果未使用磁碟加密對卸除式媒體進行加密，則儲存在此媒體上的資料需要透過其它一些方法實現不可讀性。*			
3.5 保護任何用於保全持卡人資料以防洩露和濫用的金鑰： ***註：*** *此要求也適用於保護資料加密金鑰的金鑰加密金鑰 —* *此類金鑰加密金鑰必須至少與資料加密金鑰同等強效。*	**3.5** 透過執行以下操作確認保護用於加密持卡人資料以防洩露和濫用的金鑰的程序：			
3.5.1 儘量限制僅最少人數的保管人可對加密金鑰進行存取。	**3.5.1** 檢查使用者存取清單，確認只有最少人數的必要保管人可對金鑰進行存取。			
3.5.2 採用儘可能少的位置和形式安全儲存金鑰。	**3.5.2.a** 檢查系統設定檔案，以確認金鑰以加密的形式儲存，並且金鑰加密金鑰與資料加密金鑰分開儲存。			
	3.5.2.b 確定金鑰儲存位置，以確保採用儘可能少的位置和形式安全儲存金鑰。			
3.6 對用於加密包括以下內容之持卡人資料的	**3.6.a** 確認存在用於加密持卡人資料的金鑰的金鑰管理程序。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
密碼編譯金鑰，完全記錄並實施所有金鑰管理流程和程序： ***註：*** *可以從各種途徑 (包括 NIST)獲得許多金鑰管理行業標準，具體可見於 http://csrc.nist.gov。*	**3.6.b** 僅對於服務提供商：如果服務提供商與其客戶共用金鑰來傳輸或儲存持卡人資料，則確認服務提供商向客戶提供相關文件，其中包含了有關如何按照以下要求 3.6.1 - 3.6.8 安全傳輸、儲存和更新客戶金鑰的指南。			
	3.6.c 檢查金鑰管理程序並執行以下操作：			
3.6.1 強效加密金鑰的產生	**3.6.1** 確認實施了金鑰管理程序，要求產生強效金鑰。			
3.6.2 加密金鑰的安全分發	**3.6.2** 確認執行了金鑰管理程序，以要求安全的金鑰分發。			
3.6.3 加密金鑰的安全儲存	**3.6.3** 確認執行了金鑰管理程序，以要求安全的金鑰儲存。			
3.6.4 完成加密程序之金鑰的加密金鑰變更 (例如，特定期限之後及/或特定金鑰產生特定數量的密碼文字之後)，此變更必須依照相關應用程式供應商或金鑰所有者並基於行業最佳實務與指南實施 (例如，NIST 特殊出版物 800-57)。	**3.6.4** 確認執行了金鑰管理程序，以便在定義之加密程序終端進行金鑰變更。			
3.6.5 金鑰的完整性一旦削弱 (例如，知悉純文字金鑰之員工離職)，則金鑰撤回或更換 (例如：存檔、銷毀及/或廢止) 是必要的，否則金鑰可能洩露。 ***註：*** *如果撤回或更換的加密金鑰需要保留，這些金鑰必須安全存檔 (例如使用金鑰加密金鑰)。存檔的加密金鑰僅應用於解密/驗證目的。*	**3.6.5.a** 確認在金鑰完整性削弱之後執行了金鑰管理程序以撤回金鑰。			
	3.6.5.b 確認執行了金鑰管理程序以要求更換已知或疑似洩露的金鑰。			
	3.6.5.c 如果撤回或更換的加密金鑰得以保留，則須確認這些金鑰未被用於加密作業。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
3.6.6 如果使用手動純文字加密金鑰管理作業，這些作業必須使用區段劃分知識與雙重管控措施 (例如要求兩名或三名人員重建整個金鑰，且每人僅知悉自己負責之部分金鑰)加以管理。 ***註:*** *手動金鑰管理作業範例包括但不限於:金鑰產生、傳輸、上載、儲存以及銷毀。*	**3.6.6** 確認手動純文字金鑰管理程序要求具備金鑰的區段劃分知識與雙重管控措施。			
3.6.7 防止對密碼編譯金鑰進行未經授權的替代。	**3.6.7** 確認執行了金鑰管理程序以防止對金鑰進行未經授權的替代。			
3.6.8 要求密碼編譯金鑰保管人簽署一份表單，聲明其瞭解並接受作為金鑰保管人的責任。	**3.6.8** 確認執行了金鑰管理程序，要求金鑰保管人(採用書面或電子方式) 聲明其瞭解並接受作為金鑰保管人的責任。			

要求 4：　　對在開放型公共網路之間傳輸持卡人資料進行加密

在容易被懷有惡意的人員存取的網路中傳輸敏感資訊時，必須對這些資訊進行加密。設定不當的無線網路及舊有加密和認證協定的漏洞會繼續成為惡意個體的攻擊對象，他們利用這些漏洞獲取對持卡人資料環境的權限存取。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
4.1 使用強效加密和安全協定 (例如，SSL/TLS、IPSEC、 SSH 等) 以便在開放的公用網路傳輸期間保護敏感的持卡人資料。 *PCI DSS 範疇內的開放型公共網路範例如：* ▪ Internet； ▪ 無線技術； ▪ 全球行動通訊系統 (GSM)， ▪ 通用無線分組業務 (GPRS)。	**4.1** 確認在開放型公共網絡上傳輸或接收持卡人資料時使用安全通訊協定。 確認在資料傳輸過程中使用了強效加密，如下所示：			
	4.1.a 選擇一個交易被接受並觀察其進行的樣本，確認持卡人資料在傳輸過程中進行了加密。			
	4.1.b 確認只有受信任的金鑰/證書被接受。			
	4.1.c 確認通訊協定已實施，僅使用安全設定，並且不支援不安全的版本或設定。			
	確認使用的加密方法執行了正確的加密強度。 (核查供應商建議/最佳實務。)			
	4.1.e 有關執行 SSL/TLS： ▪ 確認 HTTPS 作為瀏覽器統一記錄定位符 (URL) 的部分出現。 ▪ 確認當 HTTPS 不在 URL 中出現時不要求持卡人資料。			
4.1.1 確保傳輸持卡人資料或連接至持卡人資料環境的無線網路使用行業最佳實務 (例如 IEEE 802.11i)對驗證和傳輸實施了強效加密。 ***註：*** *嚴禁在 2010 年 6 月 30 日之前使用 WEP 作爲安全管控措施。*	**4.1.1** 對於傳輸持卡人資料或連接至持卡人資料環境的無線網路，確認使用行業最佳實務 (例如 IEEE 802.11i)對驗證和傳輸實施了強效加密。			
4.2 切勿使用最終使用者通訊技術 (例如，電子郵件、即時通訊工具、聊天工	**4.2.a** 確認 PAN 不可讀，或者在透過最終使用者通訊技術傳送 PAN 時始終使用強效加密方法進行加密。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
具等)傳送未受保護的 PAN。	**4.2.b** 確認存在聲明不透過最終使用者通訊技術傳送未加密 PAN 的政策。			

維護漏洞管理程式

要求 5：　　使用並定期更新殺毒軟體或程式

惡意軟體 (通常指「malware」，包括病毒、蠕蟲和木馬)在許多業務認證的活動中進入網路，包括員工電子郵件和 Internet、行動電腦和儲存裝置的使用，從而導致系統漏洞被利用。所有經常受惡意軟體影響的系統必須安裝使用殺毒軟體，防止受到目前和變種的惡意軟體威脅。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
5.1 在所有經常受惡意軟體影響的系統上部署殺毒軟體 (特別是個人電腦和伺服器上)。	**5.1** 對於包含所有頻繁受惡意軟體影響的作業系統類型的系統元件樣本，如果適用的殺毒技術存在，則確認是否部署了殺毒軟體。			
5.1.1 確保所有殺毒程式都能夠偵測、移除並防止所有已知類型的惡意軟體的攻擊。	**5.1.1** 對於系統元件樣本，確認所有殺毒程式偵測、移除並防止所有已知類型的惡意軟體的攻擊 (例如，病毒、木馬、蠕蟲、間諜軟體、廣告軟體和 rootkit)。			
5.2 確保所有殺毒機制都是最新且正在執行，而且能夠產生稽核日誌。	**5.2**透過執行以下各項確認所有殺毒軟體都是最新且正在執行，並且能夠產生日誌：			
	5.2.a 獲取並檢查政策，確認其要求更新殺毒軟體和定義。			
	5.2.b 確認啟用了軟體主安裝，以進行自動更新和定期掃描。			
	5.2.c 對於包含所有經常受惡意軟體影響的作業系統類型的系統元件樣本，確認啟用了自動更新和定期掃描。			
	5.2.d 對於系統元件樣本，確認啟用了殺毒軟體日誌產生功能，並且這些日誌根據 PCI DSS 要求 10.7 得到保留。			

要求 6：　　開發並維護安全系統和應用程式

懷有惡意的人員利用安全漏洞來獲取存取系統的權限。許多漏洞都能夠透過供應商提供的安全修補程式進行修復，必須由管理這些系統的機構安裝。所有關鍵系統都必須具備最新發佈的合適的軟體修補程式，以保護持卡人資料被惡意個體和惡意軟體利用和破壞。

註：
合適的軟體修補程式就是那些進行了充分評估和測試以確定這些修補程式不與現有安全設定衝突的修補程式。對於自行開發的應用程式，許多漏洞都可以透過使用標準系統開發程序和安全的編碼技術避免。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
6.1 確保所有系統元件和軟體都安裝了供應商提供的最新的安全修補程式，以防止已知漏洞造成的威脅。在發佈的一個月以內安裝關鍵的安全修補程式。 ***註：*** *組織可以考量採用基於風險的方法來設定修補程式的安裝優先權。例如，與不太關鍵的內部裝置相比，可將關鍵基礎結構 (例如，面向公眾的裝置、系統和資料庫) 的優先權設得較高，以確保優先權較高的系統和裝置能在一個月內處理完畢，而不太關鍵的裝置和系統在三個月內處理完畢即可。*	**6.1.a** 對於系統元件和相關軟體樣本，將安裝在每個系統上的安全修補程式清單與最新的供應商安全修補程式清單進行比較，以確認安裝了最新的供應商修補程式。			
	6.1.b 檢查與安全修補程式安裝相關的政策，以確認它們要求在一個月內安裝所有關鍵的新安全修補程式。			
6.2 制定一項程序，確定並指派新發現安全漏洞的風險排名。 ***註：*** ▪ *風險排名必須基於行業最佳實務。例如，排名「高」風險漏洞的標準包括達到 4.0 或以上的 CVSS 基本分數，及/或供應商提供的列爲「危急」的修補程式，及/或影響關鍵系統元件的漏洞。* ▪ *6.2.a 定義的漏洞排名在 2012 年 6 月 30 日之前被視爲最佳實務，之後它將變成一項要求。*	**6.2.a** 訪問負責之工作人員，確認已執行有關程序來確定新的安全漏洞，並且為此類安全漏洞指派風險排名。(至少，最危急、最高風險漏洞應排名為「高」。			
	6.2.b 確認用於確定新安全漏洞的程序包括使用安全漏洞資訊的外部資源。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
6.3 根據 PCI DSS (例如，安全驗證和日誌記錄) 並基於行業最佳實務，開發軟體應用程式 (內部的和外部的，包括基於 WEB 的應用程式管理存取)。將資訊安全納入整個軟體開發生命週期。這些程序必須包括以下各項：	**6.3.a** 獲取並檢查書面軟體開發程序，確認該程序是基於行業標準及/或最佳實務編制的。			
	6.3.b 檢查書面軟體開發程序，確認將資訊安全納入整個軟體開發生命週期。			
	6.3.c 檢查書面軟體開發程序，確認軟體應用程式是依照 PCI DSS 開發的。			
	6.3.d 在檢查書面軟體開發程序、訪問軟體開發者時，確認：			
6.3.1 在支付應用程式啟用或發佈給客戶之前，移除自訂的支付應用程式帳戶、使用者 ID 與密碼	**6.3.1** 在系統投入生產或發佈給使用者以前，自訂應用程式帳戶、使用者 ID 和/或密碼已移除。			
6.3.2 在發佈給生產部門或客戶之前，審查自訂程式碼，以確定任何潛在的漏洞 ***註：*** *有關程式碼審查的本要求適用於系統開發生命週期中的所有自訂程式碼 (包括內部和面向公眾的自訂程式碼)。* *程式碼審查可以由有經驗的內部工作人員或第三方進行。Web 應用程式也受到更多控制 (如果它們是面向公眾的)，以解決執行後不斷產生的威脅和漏洞，如 PCI DSS 要求 6.6 所定義的。*	**6.3.2.a** 獲取並審查政策，以確認所有自訂應用程式碼變更都必須經過審查 (使用手動或自動程序)，如下所示： ▪ 程式碼變更都必須由原始程式碼作者以外且熟知程式碼檢查技術和安全編碼實踐的人員進行。 ▪ 程式碼審查確保程式碼是根據安全的編碼指南進行開發的 (請參閱 PCI DSS 要求 6.5)。 ▪ 在發佈以前必須執行相應的更正。 ▪ 在發佈以前由管理層審查並批准程式碼檢查結果。			
	6.3.2.b 選擇最近的自訂應用程式變更的樣本，並確認自訂應用程式碼已根據上述 6.3.2.a 經過審查。			
6.4 對於系統元件進行任何變更時，遵循變更控制程序處理。這些程序必須包括以下各項：	**6.4** 在檢查變更控制程序、訪問系統與網路管理員及檢察有關資料 (網路設定文件、生產和測試資料等) 時，須確認以下各項：			
6.4.1 分開開發/測試環境與生產環境	**6.4.1** 開發/測試環境獨立於生產環境，並設定存取管控措施，以確保兩者的分離。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
6.4.2 開發/測試環境與生產環境中的職責分離	**6.4.2** 對指派到開發/測試環境與生產環境中的工作人員進行職責分離。			
6.4.3 未將生產資料 (真實的 PAN) 用於測試或開發	**6.4.3** 未將生產資料 (真實的 PAN) 用於測試或開發。			
6.4.4 在生產系統啓用之前，移除測試資料與帳戶	**6.4.4** 在生產系統啓用之前，移除測試資料與帳戶。			
6.4.5 安全修補程式和實施軟體變更的變更控制程序。該程序必須包括如下內容：	**6.4.5.a** 確認與實施安全修補程式和軟體變更相關的變更控制程序記錄在案，並確認這些程序要求下述 6.4.5.1 – 6.4.5.4 。			
	6.4.5.b 對於系統元件和最近的變更/安全修補程式樣本，將這些變更追溯至相關的變更控制記錄。對於檢查的每項變更，執行以下項目：			
6.4.5.1 影響之記錄。	**6.4.5.1** 確認每個抽樣變更的變更控制記錄包含影響記錄。			
6.4.5.2 獲得授權方的變更核准記錄。	**6.4.5.2** 確認每個抽樣變更均獲得授權方提供的核准記錄。			
6.4.5.3 測試功能，以確認變更未對系統安全造成不良影響。	**6.4.5.3.a** 對於每個抽樣的變更，確認執行功能抽樣，以確認變更未對系統安全造成不良影響。			
	6.4.5.3.b 對於自訂程式碼變更，確認在部署用於生產之前，測試所有更新對於 PCI DSS 要求 6.5 的合規性。			
6.4.5.4 取消程序。	**6.4.5.4** 確認每個抽樣變更都準備了取消程序。			
6.5 基於安全編碼指南開發應用程式 。防止軟體開發過程中出現常見編碼漏洞，並包括以下各項： ***註：*** *6.5.1 至 6.5.9 中列舉的漏洞都是此版 PCI DSS 發佈時行業最佳實務中最新的漏洞。然而，在更新漏洞管理的行業最佳實務時 (例如，OWASP 指南、SANS CWE 前 25 位、CERT 安全編碼等)，這些要求必須使用最新的最佳實務。*	**6.5.a** 獲取並審查軟體開發程序。確認程序要求基於行業最佳實務和指南對開發人員進行安全編碼技術培訓。			
	6.5.b 抽取部分開發人員進行訪問，獲取表明他們熟悉安全編碼技術的證明。			
	6.5.c. 確認這些程序已到位，以應用程式至少在以下方面沒有漏洞：			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
6.5.1 注入式漏洞，特別是 SQL 注入。同時還須考慮 OS 指令注入、LDAP 與 Xpath 注入式漏洞以及其他注入式漏洞。	**6.5.1** 注入式漏洞，特別是 SQL 注入。 (驗證輸入項，以確認使用者資料無法修改指令與查詢的意思，利用參數化查詢等。)			
6.5.2 緩衝區溢位	**6.5.2** 緩衝區溢位 (驗證緩衝區界限，截斷輸入字串。)			
6.5.3 非安全加密儲存	**6.5.3** 非安全密碼編譯儲存 (防止加密的漏洞。)			
6.5.4 非安全通訊	**6.5.4** 非安全通訊 (對所有已驗證的敏感通訊進行妥善加密。)			
6.5.5 不當錯誤處理	**6.5.5** 不當錯誤處理 (切勿透過錯誤訊息洩露資訊)			
6.5.6 漏洞識別程序確定的所有「高危」漏洞 (按照 PCI DSS 要求 6.2 的定義)。 ***註：*** *此要求在 2012 年 6 月 30 日之前被視爲最佳實務，之後它將變成一項要求。*	**6.5.6** PCI DSS 要求 6.2 定義的所有「高危」漏洞。			
註： *以下要求 6.5.7 - 6.5.9 適用於 Web 應用程式和應用程式介面 (內部或外部)：*				
6.5.7 跨網站指令碼攻擊 (XSS)	**6.5.7** 跨網站指令碼攻擊 (XSS) (在納入之前驗證所有參數，利用內容敏感的逸出等。)			
6.5.8 不當存取管控措施 (例如非安全直接物件參考，無法限制 URL 存取以及目錄傳輸)	**6.5.8** 不當存取管控措施，例如非安全直接物件參考，無法限制 URL 存取以及目錄傳輸 (正確驗證使用者並淨化輸入項。切勿向使用者公開內部物件參考。)			
6.5.9 跨網站請求偽造 (CSRF)	**6.5.9** 跨網站請求偽造 (CSRF)。(切勿答復由瀏覽器自動提交的授權證書與權杖。)			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
6.6 對於面向公眾的 Web 應用程式，經常解決新的威脅和漏洞，並確保保護這些應用程式不受到以下*任一*方法的攻擊： ▪ 透過手動或自動應用程式漏洞安全評估工具或方法檢查面向公眾的 Web 應用程式，至少每年一次並在所有變更後進行檢查 ▪ 在面向公眾的 Web 應用程式前端安裝 Web 應用程式防火牆	**6.6** 對於*面向公眾*的 Web 應用程式，確保採用了以下 *任一*方法： ▪ 確認檢查了面向公眾的 Web 應用程式 (使用手動或自動漏洞安全評估工具或方法)，如下所示： – 至少每年變更一次 – 任何變更後 – 由專門檢查應用程式安全的機構 – 所有的漏洞都被更正 – 更正後重新評估應用程式 ▪ 確認在面向公眾的 Web 應用程式前端採用了 Web 應用程式防火牆，以偵測並防止基於 Web 的攻擊。 ***註：*** *「專門檢查應用程式安全的組織」既可以是第三方公司，也可以是內部組織，只要審查者專注應用程式安全，並能證明其有區別於開發團隊的獨立性。*			

實施嚴格的存取控制措施

要求 7：　　限制為只有業務需要知道的人才能存取持卡人資料

為確保只有授權的工作人員才能存取關鍵資料，必須採用系統和程序來限制根據需要知道和工作職責進行存取。

「需要知道」是指當需要執行一項工作時授予所需之最少資料和權限的存取權利。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
7.1 限制僅工作需要之人可存取系統元件和持卡人資料。存取限制必須包括以下項目：	**7.1** 獲取並檢查資料控制書面政策，並確認政策包含以下各項：			
7.1.1 將權限使用者 ID 的存取權限限制為執行工作職責需要的最小權限	**7.1.1** 確認權限使用者 ID 的存取權限已限制為執行工作職責需要的最小權限。			
7.1.2 根據工作人員劃分和職能指派權限	**7.1.2** 確認已根據工作劃分和職能指派權限 (也被稱為「基於角色的存取控制」或 RBAC)。			
7.1.3 指定所需權限之獲得授權方的核准記錄要求。	**7.1.3** 確認所有存取均要求獲得授權方的核准記錄 (書面或電子形式)，並且還必須指定所需權限。			
7.1.4 自動存取控制系統的實施	**7.1.4** 確認透過自動存取控制系統實施了存取控制。			
7.2為多使用者系統元件建立存取控制系統，根據使用者需要知道的資料限制存取，並且設定為「禁止所有」，除非特別允許。 此存取控制系統必須包含以下各項：	**7.2** 檢查系統裝置和供應商記錄，以確認按以下方式實施了存取控制系統：			
7.2.1 涵蓋所有系統元件	**7.2.1** 確認所有的系統元件都採用了存取控制系統。			
7.2.2 根據工作劃分和職能給個人指派權限	**7.2.2** 確認存取控制系統已被設定為執行根據工作劃分和職能指派給個人的權限。			
7.2.3 預設「拒絕所有」設定 ***註：*** *一些存取控制系統被預設設定為「允許所有」，因此允許所有存取，除非制定了專門禁止的規則。*	**7.2.3** 確認存取控制系統擁有一個預設的「禁止所有」設定。			

要求 8：　　為具有電腦存取權的每個人指定唯一的 ID

為具有存取權限的每個人均指定唯一的識別碼
(ID)，以確保每個人都對自己的行為全權負責。採用此責任制之後，只有獲得授權的已知使用者才能操作重要資料和系統，而且這種操作行為可以跟蹤。

***註：** 這些要求適用於所有帶有管理功能之帳戶 (包括銷售點帳戶)，和用於檢視或存取持卡人資料或者存取帶有持卡人資料之系統的帳戶。然而，要求 8.1、8.2 和 8.5.8 - 8.5.15 並不適用於銷售點支付應用程式的使用者帳戶，為便於單次交易 (例如出納帳戶)，這些帳戶每次僅可存取一個卡號。*

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
8.1 在允許所有使用者存取系統元件或持卡人資料之前為其指派唯一的 ID。	**8.1確定已為所有使用者指派用於存取系統元件或持卡人資料的唯一 ID。**			
8.2除指派唯一的 ID 之外，至少採用以下一種方法驗證所有使用者的身份： ▪ 您知道的東西，例如密碼或口令 ▪ 您擁有的東西，例如象徵性裝置或智慧卡 ▪ 您的身份描述，例如生物識別資訊	**8.2** 要使用唯一的 ID 和其他驗證方法 (例如密碼)來確認使用者已經過驗證並可存取持卡人資料環境，請執行下列操作： ▪ 獲取描述所用驗證方法的文件並進行檢查。 ▪ 對於使用的每一種驗證方法和每一種系統元件，觀察驗證操作以確定其運作與記錄的驗證方法相一致。			
8.3 員工、管理員和第三方採用雙因素驗證對網路的遠端存取 (從網路外進行網路層級的存取)進行驗證。(例如，遠端驗證和帶有權杖的撥入服務 (RADIUS)；終端存取控制器、存取帶有權杖的存取控制系統 (TACACS)；或者便於雙因素驗證的其他技術。) ***註：*** *雙因素驗證要求使用三種驗證方法之中的兩種方法進行驗證 (請參閱要求 8.2 的驗證方法描述)。兩次使用一種因素 (例如使用兩個單獨的密碼) 不被視爲雙因素驗證。*	**8.3** 為確認對所有遠端網路存取實施了雙因素驗證，觀察一名員工 (例如管理員)遠端連接至網路並確認其使用了三種驗證方法中的兩種方法。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
8.4 在所有系統元件上進行傳輸和儲存操作時，使用強效加密使所有密碼不可讀。	**8.4.a** 對於系統元件樣本，檢查密碼檔案以確認密碼在傳輸和儲存過程中不可讀取。			
	8.4.b 僅對服務提供商而言，請檢查密碼檔案以確認客戶密碼得到加密。			
8.5 確保在所有系統元件上都對非消費者使用者和管理員使用正確的使用者身份識別和驗證管理，具體如下：	**8.5** 透過執行下列操作審查程序和訪問相關工作人員，確認實施了使用者身份識別和驗證管理程序：			
8.5.1 控制使用者 ID、認證和其他識別物件的增加、刪除和修改操作。	**8.5.1** 抽樣選擇使用者 ID，包括管理員和普通使用者。透過執行下列操作，確認每位使用者獲得授權並可根據政策使用系統： ▪ 獲取每個 ID 的授權表並予以檢查。 ▪ 透過跟蹤從授權表到系統的資訊，檢查抽樣的使用者 ID 是否能夠根據授權表(包括根據指定的權限和所有獲取的簽名)實施操作。			
8.5.2 重設密碼前確認使用者身份。	**8.5.2** 檢查密碼/驗證程序並觀察安全工作人員，以確認使用者在透過電話、電子郵件、網路或其他非面對面方式請求重設密碼時，先驗證使用者身份再重設密碼。			
8.5.3 為每位使用者的首次使用設定密碼，然後重設為唯一值，並在首次使用後立即變更。	**8.5.3** 檢查密碼程序並觀察安全工作人員，以確認每位新使用者的初始密碼和現有使用的重設密碼都被設定為唯一值，並且首次使用後都會變更。			
8.5.4 對所有已終止的使用者立即撤銷其存取權限	**8.5.4** 抽樣選擇過去六個月中已終止的使用者，審查目前的使用者存取清單 ，以確認他們的 ID 已被停用或移除。			
8.5.5 至少每 90 天移除/停用一次非活躍的使用者帳戶。	**8.5.5** 確定處於非活躍狀態超過 90 天的帳戶已被移除或停用。			
8.5.6 僅在需要時啓用供應商用於遠端存取的帳戶。密切監視供應商對遠端存取帳戶的使用。	**8.5.6.a** 確認供應商用於存取、支援和維護系統元件的所有帳戶均已停用，並僅在供應商需要時啟用。			
	8.5.6.b 確認供應商遠端存取帳戶在使用時受到監視。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
8.5.7 與存取持卡人資料的所有使用者溝通驗證程序和政策。	**8.5.7** 訪問使用者 ID 樣本內的使用者，以確認他們熟悉驗證程序和政策。			
8.5.8 切勿使用群組、共用或一般帳戶和密碼或者其他驗證方法。	**8.5.8.a** 對於系統元件樣本，檢查使用者 ID 清單以確認下列內容： ▪ 一般使用者 ID 和帳戶已停用或移除。 ▪ 用於系統管理活動和其他重要功能的共用使用者 ID 已不存在 ▪ 共用使用者 ID 和一般使用者 ID 未用於管理任何系統元件			
	8.5.8.b 檢查驗證政策/程序，確認群組和共用密碼或其他驗證方法受到明確禁止。			
	8.5.8.c訪問系統管理員，以確認尚未分配群組和共用密碼或其他驗證方法，即使已有請求。			
8.5.9 至少每 90 天變更一次使用者密碼。	**8.5.9.a**對於系統元件樣本，獲取系統組態設定並進行檢查，以確認使用者密碼參數被設定為要求使用者至少每 90 天變更一次密碼。			
	8.5.9.b 僅對於服務提供商而言，審查內部程序和客戶/使用者文件，以確認非消費者使用者密碼需要定期變更，並確認所有非消費者使用者都會獲得何時、在何種情況下必須變更密碼的指導說明。			
8.5.10 密碼長度必須至少達到七個字元。	**8.5.10.a** 對於系統元件樣本，獲取系統組態設定並進行檢查 ，以確認密碼參數被設定為要求密碼長度至少達到七個字元。			
	8.5.10.b 僅對於服務提供商而言，檢查內部程序和客戶/使用者文件，以確認非消費者使用者密碼被要求符合最低長度要求。			
8.5.11 使用包含數字和字母字元的密碼。	**8.5.11.a** 對於系統元件樣本，獲取系統組態設定並進行檢查，以確認密碼參數被設定為要求密碼包含數字和字母字元。			
	8.5.11.b 僅對於服務提供商而言，審查內部程序和客戶/使用者文件，以確認非消費者使用者密碼被要求包含數字和字母字元。			
8.5.12 切勿允許個人提交和其前四次使用過的	**8.5.12.a** 對於系統元件樣本，獲取系統組態設定並進行檢查，以確認密碼參			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
任意密碼相同的新密碼。	數被設定為要求新密碼不能和前四次使用過的密碼相同。			
	8.5.12.b 僅對於服務提供商而言，審查內部程序和客戶/使用者文件，以確認非消費者使用者密碼不能和前四次使用的密碼相同。			
8.5.13 透過鎖定六次嘗試之後的使用者 ID，限制反復存取嘗試。	**8.5.13.a** 對於系統元件樣本，獲取系統組態設定並進行檢查，以確認驗證參數被設定為要求使用者帳戶在六次無效登入嘗試之後被鎖定。			
	8.5.13.b 僅對於服務提供商而言，審查內部程序和客戶/使用者文件，以確認非消費者使用者帳戶在六次無效登入嘗試之後被鎖定。			
8.5.14 將鎖定時長設定為至少 30 分鐘或直到管理員啟用該使用者 ID 為止。	**8.5.14** 對於系統元件樣本，獲取系統組態設定並進行檢查，以確認密碼參數被設定為要求使用者帳戶一旦鎖定後會至少鎖定 30 分鐘，或者直到系統管理員重設該帳戶才解除鎖定。			
8.5.15 如果工作階段保持閒置狀態超過 15 分鐘，則要求使用者重新驗證以重新啟動終端或工作階段。	**8.5.15** 對於系統元件樣本，獲取系統組態設定並進行檢查，以確認系統/工作階段的閒置狀態超時時間已設定為 15 分鐘或更少。			
8.5.16 驗證對包含持卡人資料的任何資料庫的所有存取。這包括應用程式、管理員和所有其他使用者的存取操作。 限制僅資料庫管理員可執行資料庫的使用者直接存取或查詢。	**8.5.16.a** 審查資料庫和應用程式組態設定，確認在存取之前驗證所有使用者。			
	8.5.16.b 確認資料庫和應用程式組態設定確保所有的使用者存取資料庫、查詢資料庫和操作資料庫 (例如移動、複製、刪除) 行為必須僅透過程式設計方法實施 (例如，透過儲存的程序)。			
	8.5.16.c 確認資料庫和應用程式組態設定限制僅資料庫管理員可執行資料庫的使用者直接存取或查詢。			
	8.5.16.d 審查資料庫應用程式和相關應用程式 ID，以確認應用程式 ID 僅限應用程式 (而不是個人使用者或其他程序) 使用。			

要求 9：　　限制對持卡人資料的實際存取

任何實體存取資料或儲存持卡人資料的系統的操作，都會為個人提供存取裝置或資料並移除系統或複本的機會，這種行為應受到適當限制。出於要求 9
之目的，「現場工作人員」指的是全職和兼職雇員、臨時雇員和承包商以及實際出現在實體場所的顧問。「訪客」是指供應商、任何現場工作人員的客人、服務人員或需要進入場所作短暫停留 (通常不超過一天) 的任何人。「媒體」是指包含持卡人資料的所有紙質和電子媒體。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
9.1 使用適當的設施進入管控措施，以限制和監控在持卡人資料環境中對系統的實體存取。	**9.1** 確認持卡人資料環境中的每間電腦室、資料中心和其他帶有系統的實體區域都設有實體安全管控措施。 ▪ 確認已使用識別證讀取機或其他裝置 (包括獲得授權的識別證、鎖和金鑰)控制存取。 ▪ 觀察系統管理員嘗試在持卡人環境中登入隨意選擇的系統主控台時的操作，確定這些主控台已「鎖定」，以防止未經授權的使用。			
9.1.1 使用攝影機及/或存取控制機制，以監控個人對敏感區域的實體存取。檢查收集的資料並與其他入口相關聯。至少儲存三個月，法律另有規定者除外。 ***註：*** *「敏感區域」是指用於儲存、處理或傳輸持卡人資料的系統所在的任何資料中心、伺服器室或任何區域。其中不包括只有銷售點終端的區域，例如零售店中的收銀區。*	**9.1.1.a** 確認攝影機及/或存取控制機制已到位，可監控敏感區域的入口/出口。			
	9.1.1.b 確認攝影機及/或存取控制機制不會受到篡改或停用。			
	9.1.1.c 確認攝影機及/或存取控制機制已受到監控，而且攝影機或其他機制中的資料至少儲存三個月。			
9.1.2 限制對公共存取網路端子的實體存取。例如，訪客可存取區域不得啓用網路連接埠，除非網路存取獲得明確授權。	**9.1.2** 透過訪問網路管理員並進行觀察，以確認網路端子僅在獲得授權之現場工作人員需要時才會啟用。此外，在這些網路插座交換機處於活躍狀態的區域，應確定訪客身邊始終都有陪護人員。			
9.1.3 限制對於無綫存取點、閘道、掌上型裝置、網路/通訊硬體和電信綫的實體存取。	**9.1.3** 確認正確限制對於無綫存取點、閘道、掌上型裝置、網路/通訊硬體和電信綫的實體存取。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
9.2 制訂相關程序，以迅速識別現場工作人員和訪客，尤其是在可以存取持卡人資料的區域迅速識別雇員和訪客。	**9.2.a** 審查向現場工作人員和訪客指派識別證的程序，並確認這些程序包括以下內容： ▪ 授予新識別證， ▪ 變更存取要求，以及 ▪ 撤銷終止關係的現場工作人員和過期的訪客識別證			
	9.2.b 確認僅有獲得授權之工作人員可存取識別證系統。			
	9.2.c 檢查在用之識別證，確認其可清楚識別訪客，並且現場工作人員和訪客可輕易識別。			
9.3 確保按照如下要求處理所有訪客的來訪：	**9.3** 確認已佈署訪客管控措施，具體如下：			
9.3.1 須經授權方可進入處理或維護持卡人資料的區域。	**9.3.1** 觀察訪客 ID 識別證的使用情況，以確認訪客 ID 識別證在無人陪同的情況下不允許對儲存持卡人資料的實體區域進行存取。			
9.3.2 提供可以將訪客識別為非現場工作人員而且使用後會過期的實體權杖(例如識別證或存取裝置)。	**9.3.2.a** 觀察設施之內的人，以確認訪客佩戴訪客 ID 識別證，並且可輕易識別訪客和現場工作人員。			
	9.3.2.b 確認訪客識別證已過期。			
9.3.3 要求訪客在離開設施前或實體權杖到期時交出實體權杖。	**9.3.3** 觀察要離開設施的訪客，以確認要求訪客在離開時或識別證過期時交出訪客 ID 識別證。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
9.4 使用訪客日誌，以維護訪客活動的實體稽核記錄。在日誌上記錄訪客姓名、所屬公司以及授權訪客實體存取的現場工作人員。將該日誌至少保留三個月，法律另有規定者除外。	**9.4.a** 確認已使用訪客日誌，以記錄對儲存或傳輸持卡人資料的設施、電腦室以及資料中心的實體存取活動。			
	9.4.b 確認日誌包含訪客姓名、所屬公司以及授權訪客實體存取的現場工作人員，並且該日誌至少保留三個月。			
9.5 將備份媒體儲存在安全的地方，最好是在異地設施，例如替代或備用場所、或商業儲存設施。至少每年審查一次該場所的安全性。	**9.5.a** 觀察儲存之地的實體安全狀況，以確認備份媒體儲存是安全的。			
	9.5.b 確認儲存之地的安全至少每年審查一次。			
9.6 以實體方式保護所有媒體的安全。	**9.6** 確認保護持卡人資料的程序包括保護所有媒體(包括但不限於電腦、卸除式電子媒體、紙本收據、紙本報告和傳真)的管控措施。			
9.7 始終嚴格控制在內部或外部分發任何類型的媒體，包括以下內容：	**9.7** 確認已制訂控制分發媒體的政策，並確認此政策涵蓋所有分發的媒體(包括向個人分發的媒體)。			
9.7.1 分類媒體，以便確定資料的敏感性。	**9.7.1** 確認對所有媒體進行分類，以便確定資料的敏感性。			
9.7.2 使用安全的快遞服務或其他可準確跟蹤的傳送方法傳送媒體。	**9.7.2** 確認所有傳送到設施之外的媒體都已記錄並獲得管理層授權，而且傳送時都使用了安全的快遞服務或其他可準確跟蹤的傳送方法。			
9.8 將任何和所有媒體從安全區域轉移時(尤其是將媒體發放給個人時)，務必確保獲得管理層同意。	**9.8** 選擇所有媒體最近幾天的異地跟蹤日誌樣本，確認日誌中有跟蹤詳情和相應的管理層授權記錄。			
9.9 嚴格控制對媒體的儲存和存取	**9.9** 獲取控制所有媒體儲存和維護的政策並進行檢查，以確認此政策要求媒體定期盤存。			
9.9.1 正確維護所有媒體的盤存日誌，並且媒體至少每年盤存一次。	**9.9.1** 獲取媒體盤存日誌並進行審查，以確認媒體定期盤存至少每年執行一次。			
9.10 銷毀因業務或法律原因不再需要的媒體，具體如下：	**9.10** 獲取媒體定期銷毀的政策並進行檢查，以確認該政策涵蓋所有媒體，並確認以下項目：			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
9.10.1 對實體複本材料進行粉碎、焚燒或打漿，以致持卡人資料無法復原。	**9.10.1.a** 確認對實體複本材料進行橫切粉碎、焚燒或打漿，以合理保證這些實體複本材料無法復原。			
	9.10.1.b 檢查用來銷毀資訊的儲存容器，以確認這些容器的安全性。例如，確認「待粉碎」容器上有鎖，以防止他人查看容器中的內容。			
9.10.2 使電子媒體上的持卡人資料不可恢復，以確保持卡人資料無法復原。	**9.10.2** 確認依照行業認可的安全刪除標準，使用安全擦除程序，促使電子媒體上的持卡人資料無法恢復，或者使用其他實體方法銷毀媒體(例如消磁)。			

定期監控並測試網路

要求 10： 追蹤並監控對網路資源及持卡人資料的所有存取

記錄機制和跟蹤使用者活動的功能對於預防、偵測和消除資料洩漏的不良影響至關重要。在所有環境中使用日誌可在出現問題時詳細地跟蹤、發出警報並進行分析。沒有系統活動日誌，確定問題根源會變得異常困難 (如果並非不可能)。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
10.1 制定一項程序以實現所有系統元件 (尤其是具有根權限等管理權限的存取)之存取與每個個人使用者的連結。	**10.1** 透過觀察和訪問系統管理員，確認稽核記錄已啟用並處於活躍狀態，可用於系統元件。			
10.2 針對所有系統元件實施自動稽核記錄，以重建以下事件：	**10.2** 透過檢查訪問、稽核日誌和稽核日誌設定，執行以下項目：			
10.2.1 對持卡人資料的所有個人存取	**10.2.1** 確認記錄所有個人存取持卡人資料的操作。			
10.2.2 具有根權限或管理權限的任何個人實施的所有操作	**10.2.2** 確認記錄具有根權限或管理權限的任何個人實施的操作。			
10.2.3 對所有稽核記錄的存取	**10.2.3** 確認記錄所有稽核記錄的存取操作。			
10.2.4 無效的邏輯存取嘗試	**10.2.4** 確認記錄無效的邏輯存取嘗試。			
10.2 5 身份識別和驗證機制的使用	**10.2.5** 確認記錄身份識別和驗證機制的使用情況。			
10.2.6 稽核記錄的初始化	**10.2.6** 確認記錄稽核日誌的初始化。			
10.2.7 系統層級物件的建立和刪除	**10.2.7** 確認記錄系統層級物件的建立和刪除。			
10.3 針對每個事件的所有系統元件至少記錄以下稽核記錄項目：	**10.3** 透過訪問和觀察，針對每個可稽核事件 (參閱 10.2)，執行以下內容：			
10.3.1 使用者身份識別	**10.3.1** 確定日誌項目中包括使用者身份識別。			
10.3.2 事件類型	**10.3.2** 確認日誌項目中包括事件類型。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
10.3.3 日期和時間	**10.3.3** 確認日誌項目中包括日期和時間戳記。			
10.3.4 成功或失敗指示	**10.3.4** 確認日誌項目中包括成功指示或失敗指示。			
10.3.5事件起源	**10.3.5**確認日誌項目中包括事件起源。			
10.3.6 受影響資料、系統元件或資源的識別碼或名稱	**10.3.6** 確認日誌項目中包括受影響資料、系統元件或資源的識別碼或名稱。			
10.4 使用時間同步處理技術，使所有關鍵系統時鐘和時間實現同步，並確保執行以下各項來擷取、分發和儲存時間。 ***註：****時間同步處理技術的一則範例是網路時間協定 (NTP)。*	**10.4.a** 確認按照 PCI DSS 要求 6.1 和 6.2 實施時間同步處理技術並及時更新。			
	10.4.b 獲取並審查在組織內部擷取、分發和儲存正確時間的程序，並且審查系統元件樣本的時間相關系統參數設定。確認程序中包括以下內容並且能夠全部實施：			
10.4.1 關鍵系統的時間正確且一致。	**10.4.1.a** 確認僅指定的中央時間伺服器接收外部來源的時間信號，並且外部來源的時間信號是基於國際不可部分完成時間或 UTC。			
	10.4.1.b 確認指定的中央時間伺服器彼此對等，以維持精確的時間，並且其他內部伺服器僅接收來自中央時間伺服器的時間。			
10.4.2 時間資料受到保護。	**10.4.2.a** 審查系統組態和時間同步設定，確認僅限制有存取時間資料之業務需求的工作人員可存取時間資料。			
	10.4.2.b 審查系統組態和時間同步設定與程序，確認關鍵系統之時間設定的任何變更均會被記錄、監視和審查。			
10.4.3 接受來自行業認可之時間來源的時間設定。	**10.4.3** 確認時間伺服器接受來自特定的行業認可之外部來源時間更新 (以防止個人惡意變更時鐘)。或者，可使用對稱金鑰加密這些更新，而且可建立存取控制清單，以指定客戶端機器的 IP 位址和時間更新一起提供 (以防止未經授權使用內部時間伺服器)。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
10.5 保護稽核記錄，使其無法變更。	**10.5**訪問系統管理員並檢查權限，確認稽核記錄已處於保護狀態，無法變更，具體如下：			
10.5.1 僅限出於工作需要的人員檢視稽核記錄。	**10.5.1** 確認 只有出於工作需要的個人才可檢視稽核記錄檔案。			
10.5.2 保護稽核記錄檔案，以防未經授權的修改。	**10.5.2** 確認 已透過存取控制機制、實體隔離和/或網路隔離保護目前的稽核記錄檔案，以防未經授權的修改。			
10.5.3 將稽核記錄檔案迅速備份到難以篡改的中心日誌伺服器或媒體。	**10.5.3** 確認 目前的稽核記錄檔案已迅速備份到難以篡改的中心日誌伺服器或媒體。			
10.5.4 將面向外部之技術的日誌寫入內部 LAN 上的日誌伺服器。	**10.5.4** 確認 面向外部之技術 (例如無線、防火牆、DNS、郵件)的日誌已卸載或複製到安全的內部中心日誌伺服器或媒體。			
10.5.5 針對日誌使用檔案完整性監控軟體或變更偵測軟體，以確保現有的日誌資料在未產生警報的情況下不會變更 (儘管增加新資料不會引發警報)。	**10.5.5** 檢查系統設定、受監控的檔案以及監控活動得出的結果，確認針對日誌使用了檔案完整性監控軟體或變更偵測軟體。			
10.6 至少每天審查一次所有系統元件的記錄。日誌審查必須包括檢查執行入侵偵測系統 (IDS) 等安全功能的伺服器和驗證、授權以及記帳協定 (AAA) 伺服器 (例如 RADIUS)。 ***註：*** *使用日誌收集工具、分析工具和報警工具，以達到根據「要求 10.6」的合規性規定。*	**10.6.a** 獲取安全政策和程序並進行檢查，以確認它們包括至少每天審查一次安全日誌的程序，同時確認它們要求在例外的情況下跟蹤後續事項。			
	10.6.b 透過觀察和訪問，確認所有系統元件都會執行定期日誌審查。			
10.7 稽核記錄歷史至少保留一年，並且至少 (例如線上、已歸檔或從備份中可恢復的)	**10.7.a** 獲取安全政策和程序並進行檢查，以確認它們包括稽核日誌保留政策，而且它們要求稽核日誌至少保留一年。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
三個月的歷史記錄可立即用於分析。	**10.7.b** 確認稽核日誌至少保留一年以備用，並且已制訂程序用於立即恢復至少前三個月的日誌以供分析。			

要求 11：　　定期測試安全系統和程序。

懷有惡意的人員和研究人員不斷發現新的漏洞，新的軟體亦在不斷引入新的漏洞。因此應經常測試系統元件、程序和自訂軟體，以確保根據不斷變化的環境不斷實施安全控制。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
11.1 測試無綫存取點的存在，定期偵測未經授權的無綫存取點。 ***註：*** *程序可用的方法包括但不限於無綫網路掃描、系統元件和基礎結構的實體/邏輯檢查、網路存取控制 (NAC) 或無綫 IDS/IPS。* *無論使用何種方法，它們都必須足以偵測並識別任何未經授權的裝置。*	**11.1.a** 確認實體設有記錄程序，用於每季偵測並識別一次無綫存取點。			
	11.1.b 確認所用方法足以偵測並識別任何未經授權的無綫存取點，至少包括以下項目： ▪ 插入系統元件的 WLAN 卡 ▪ 連接至系統元件的可攜式無綫裝置 (例如，透過 USB 等) ▪ 連接至網路連接埠或網路裝置的無綫裝置			
	11.1.c 確認用於識別未經授權之無綫存取點的記錄程序至少每季針對系統元件和設施實施一次。			
	11.1.d 如果使用自動監控 (例如，無綫 IDS/IPS、NAC 等)，則確認設定會及時警示相關工作人員。			
	11.1.e 確認組織的事故回應計劃 (請參閱「要求 12.9」) 包括在偵測到未經授權的無線裝置時予以回應。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
11.2 至少每季度以及 在網路有任何重大變更後 (例如新的系統元件安裝、網路拓撲變更、防火牆規則修改、產品更新)執行一次內部和外部網路漏洞掃描。 ***註：*** *如果評估商確定以下內容，則不要求必須完成四次通過性季度掃描才能獲得初始的 PCI DSS 遵從性：1)* *最近一次的掃描結果成功通過：2)* *機構已記錄了要求季度掃描的政策和程序；以及 3)* *掃描結果中指出的漏洞在重新掃描時顯示已糾正。第一次 PCI DSS 檢查完成之後的年份中，必須執行四次通過性季度掃描。*	**11.2** 確認按照以下程序執行內部和外部漏洞掃描：			
11.2.1 執行內部漏洞季度掃描。	**11.2.1.a** 審查掃描報告並確認在最近 12 個月內執行了四次內部季度掃描。			
	11.2.1.b 審查掃描報告並確認掃描程序包含重新掃描，直至成功通過為止，或者 PCI DSS 要求 6.2 定義之所有「高危」漏洞均得到解決。			
	11.2.1.c 驗證執行掃描的是具有相關資質的內部人員或外部第三方，如有可能，還應確保測試方的組織獨立性 (不必為 QSA 或 ASV)。			
11.2.2 每季度的外部漏洞掃描必須由支付卡行業安全標準協會 (PCI SSC) 認可的核准掃描供應商 (ASV) 執行。 ***註：****每季度的外部漏洞掃描必須由支付卡行業安全標準協會 (PCI SSC) 認可的核准掃描供應商 (ASV)*	**11.2.2.a** 審查最近四個季度的外部漏洞掃描輸出結果，並確認四次季度掃描發生在最近 12 個月內。			
	11.2.2.b 審查每次季度掃描的結果，以確保符合「ASV 計劃指南」的要求 (例如，不存在 CVSS 評級超過 4.0 的漏洞和自動失效)。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
執行。網路變更後執行的掃描可由內部人員執行。	**11.2.2.c** 審查掃描報告，以確認掃描由支付卡行業安全標準協會 (PCI SSC) 認可的核准掃描供應商 (ASV) 完成。			
11.2.3 每次出現重大變更之後立即執行內部和外部掃描。 ***註：*** *變更後執行的掃描可由內部人員執行。*	**11.2.3.a** 檢查變更控制文件和掃描報告，確認每次重大變更之後都會對系統元件進行掃描。			
	11.2.3.b 審查掃描報告並確認掃描程序包含重新掃描，直至： ▪ 對於外部掃描，不存在得分超過 CVSS 評級為 4.0 的漏洞， ▪ 對於內部掃描，可成功通過，或者 PCI DSS 要求 6.2 定義之所有「高危」漏洞均得到解決。			
	11.2.3.c 驗證執行掃描的是具有相關資質的內部人員或外部第三方，如有可能，還應確保測試方的組織獨立性 (不需要為 QSA 或 ASV)。			
11.3 外部和內部滲透測試每年至少執行一次，基礎結構或應用程式有任何重大升級或修改後 (例如作業系統升級、環境中增加子網路或環境中增加網路伺服器)也應執行。此類滲透測試必須包括以下內容：	**11.3.a**獲取最近的滲透測試結果並進行檢查，以確認該滲透測試至少每年執行一次，而且在環境發生任何重大變動後都會執行。			
	11.3.b 確認記錄的可被利用的漏洞都已糾正並且測試多次重複執行。			
	11.3.c 確認執行測試的是具有相關資質的內部人員或外部第三方，如有可能，還應確保測試方的組織獨立性 (不需要為 QSA 或 ASV)。			
11.3.1 網路層滲透測試	**11.3.1** 確認滲透測試包括網路層滲透測試。此類測試應包括支援網路功能和作業系統的元件。			
11.3.2 應用程式層滲透測試	**11.3.2** 確認滲透測試包括應用程式層滲透測試。此類測試至少應包括要求 6.5 列舉的漏洞。			
11.4 使用入侵偵測系統和/或入侵防禦系統，以監控持卡人資料環境周邊及其內部關鍵點	**11.4.a** 確認已使用入侵偵測系統和/或入侵防禦系統，並確認持卡人資料環境周邊及其內部關鍵點的所有流量都處於監控之下。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
的所有流量，並在發現可疑威脅時提醒工作人員。 隨時更新所有入侵偵測引擎和入侵防禦引擎、基準和簽名。	**11.4.b** 確定 IDS 和/或 IPS 被設定為一旦發現可疑威脅即提醒工作人員。			
	11.4.c 檢查 IDS/IPS 設定並確定 IDS/IPS 裝置已根據供應商的說明進行設定、維護和更新，以確保最佳的防護效能。			
11.5 部署檔案完整性監控工具，一旦發現關鍵系統檔案、組態檔案或內容檔案未經授權的修改即提醒工作人員；設定該軟體，使其至少每週比較一次重要檔案。 ***註：*** *在談及檔案完整性監控時，關鍵檔案通常是指那些不常變更但一經修改便可能表明系統受到威脅或可能受到威脅的檔案。相關作業系統的關鍵檔案通常會配備預先設定的檔案完整性監控產品。其他的重要檔案* *(例如自訂應用程式的檔案)則必須由機構(即商戶或服務提供商)來評估和定義。*	**11.5.a** 觀察系統設定和受監控的檔案，同時審查監控活動結果，以確認持卡人資料環境中已使用檔案完整性監控工具。 需要監控的檔案範例： ▪ 系統可執行檔 ▪ 應用程式可執行檔 ▪ 組態檔案和參數檔案 ▪ 集中儲存的、歷史的或封存的日誌檔案和稽核檔案			
	11.5.b 確認工具已設定為，一旦發現重要檔案遭受未經授權的修改即提醒工作人員，並且至少每週比較一次重要檔案。			

維護資訊安全政策

要求 12：維護處理適用於所有工作人員之資訊安全的政策。

強有力的安全政策會為整個實體設定安全基調，使工作人員瞭解應該如何去做。所有工作人員都應瞭解資料的敏感性以及他們負有保護資料的責任。出於要求 12 之目的，「工作人員」指的是全職和兼職雇員、臨時雇員、承包商以及「常駐」在實體場所或者進出持卡人資料環境的顧問。

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
12.1 建立、發佈、維護和散佈可完成以下各項操作的安全政策：	**12.1** 檢查資訊安全政策，確認該政策已發佈並散佈給所有相關工作人員(包括供應商和業務合作夥伴)。			
12.1.1 處理所有 PCI DSS 要求。	**12.1.1** 確認政策可處理所有 PCI DSS 要求。			
12.1.2 包括識別威脅和漏洞並能產生正式風險評估的年度程序。 (風險評估方法的範例包括但不限於 OCTAVE、ISO 27005 和 NIST SP 800-30。)	**12.1.2.a** 確認識別威脅和漏洞並能產生正式風險評估的年度風險評估程序得到記錄。			
	12.1.2.b 審查風險評估文件，以確認風險評估程序至少每年執行一次。			
12.1.3 包括至少每年執行一次審查，並在環境變更時及時更新。	**12.1.3** 確認資訊安全政策至少每年審查一次，並在需要時進行更新以反映業務目標或風險環境的變更。			
12.2 根據此規格中的要求制訂每日作業安全程序 (例如，使用者帳戶維護程序和日誌審查程序)。	**12.2** 檢查每日作業安全程序。確認它們符合此規格，並且包括管理程序和技術程序以符合每一項要求。			
12.3 針對重要技術 (例如，遠端存取技術、無線技術、卸除式電子媒體、筆記型電腦、平板、個人資料/數位助理 (PDA)、電子郵件使用和網際網路使用)制訂使用政策，並定義這些技術得正確使用方法。確保此類使用政策要求以下內容：	**12.3** 獲取重要技術的使用政策並進行檢查，然後執行以下程序：			
12.3.1 獲得授權方的明確核准	**12.3.1** 確認使用政策要求來自獲得授權方對於使用此類技術的明確核准。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
12.3.2 針對技術使用的驗證	**12.3.2** 確認使用政策要求所有技術在使用時必須接受使用者 ID 和密碼或其他授權項目 (例如權杖)驗證。			
12.3.3 所有此類裝置和獲得存取權之工作人員清單	**12.3.3** 確認使用政策要求提供所有裝置和獲授權使用此類裝置之工作人員清單。			
12.3.4 在裝置上黏貼標籤以確定所有者、聯絡資訊和用途	**12.3.4** 確認使用政策要求在裝置上黏貼標籤並注明所有者、聯絡資訊及用途。			
12.3.5 可接受的技術用途	**12.3.5** 確認使用政策要求提供可接受的技術使用方式。			
12.3.6 針對這些技術的可接受網路位置	**12.3.6** 確認使用政策要求提供可接受的技術網路位置。			
12.3.7 公司認可的產品清單	**12.3.7** 確認使用政策要求提供公司認可的產品清單。			
12.3.8 在非活躍狀態達到特定時限後，自動中斷遠端存取技術的工作階段	**12.3.8** 確認使用政策要求非活躍狀態達到特定時限後自動中斷遠端存取技術的工作階段。			
12.3.9 僅在供應商和商業合作夥伴需要時為其啓用遠端存取技術，並在使用之後立即停用	**12.3.9** 確認使用政策僅在供應商和商業合作夥伴需要時為其啓用遠端存取技術，並在使用之後立即停用。			
12.3.10 對於透過遠端存取技術存取持卡人資料的工作人員，禁止將持卡人資料複製、移動和儲存到本機硬碟和卸除式電子媒體，除非因定義清晰之業務需求而獲得明確授權。	**12.3.10.a** 確認使用政策禁止在透過遠端存取技術存取持卡人資料時將此類資料複製、移動和儲存到本機硬碟和卸除式電子媒體。			
	12.3.10.b 對於獲得適當授權的工作人員，確認使用政策要求按照 PCI DSS 要求保護持卡人資料。			
12.4 確保安全政策和程序明確定義了所有工作人員的資訊安全職責。	**12.4** 確認資訊安全政策已明確定義了所有工作人員的資訊安全職責。			
12.5 針對個人或團隊指派以下資訊安全管理職責：	**12.5** 確認已向首席安全執行長或其他具有安全知識的管理層成員正式指派資訊安全職責。 獲取資訊安全政策和程序並進行檢查，確認已透過正式管道明確指派了以下資訊安全職責：			
12.5.1 建立、記錄和分發安全政策和程序。	**12.5.1** 確認建立、分發安全程序和程序的職責已正式指派。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
12.5.2 監控、分析安全警報和安全資訊並將其分發給相關工作人員。	**12.5.2** 確認已正式指派監控、分析安全警報並將資訊分發給相關資訊安全部和業務部管理層人員的職責。			
12.5.3 建立、記錄和分發安全事故回應和逐層上報程序，確保及時有效地處理所有情況。	**12.5.3** 確認建立、分發安全事故回應和逐層上報程序的職責已正式指派。			
12.5.4 管理使用者帳戶，包括新增、刪除和修改	**12.5.4** 確認管理使用者帳戶和驗證管理的職責已正式指派。			
12.5.5 監控和控制所有資料存取。	**12.5.5** 確認監控和控制所有資料存取的職責已正式指派。			
12.6 實施正式的安全意識計劃，使所有工作人員都能瞭解持卡人資料安全的重要性。	**12.6.a** 確認已針對所有工作人員部署了正式的安全意識計劃。			
	12.6.b 獲取安全意識計劃的程序和文件並進行檢查，然後執行以下各項：			
12.6.1 在入職時教育工作人員並且每年執行一次教育培訓。 ***註：*** *教育方法可多種多樣，具體取決於工作人員的角色及其存取持卡人資料的層級。*	**12.6.1.a** 確認安全意識計劃可提供與工作人員溝通安全意識、教育工作人員的多種方法 (例如海報、信函、備忘錄、基於網路的培訓、會議和宣傳)。			
	12.6.1.b 確認工作人員在入職時參加安全意識培訓，而且此後每年至少參加一次。			
12.6.2 要求工作人員每年至少確認一次他們已閱讀並瞭解安全政策和程序。	**12.6.2** 確認安全意識計劃要求工作人員每年至少確認 (以書面方式或電子方式)一次他們已閱讀並瞭解資訊安全政策。			
12.7 在錄用之前甄選潛在工作人員，以最大程度降低內部來源攻擊的風險。 (背景調查的範例包括以前的雇用歷史、犯罪記錄、信用歷史和證明人調查。) ***註：*** *對於將被特定職位錄用的潛在工作人員(如在促成交易時一次只能存取一個卡號的商店收銀員)，本要求僅為建議。*	**12.7**詢問人力資源部管理層，確認在錄用可存取持卡人資料或持卡人資料環境的潛在工作人員之前針對他們實施過背景調查 (符合當地法律規定)。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
12.8 如果持卡人資料與服務提供商共用，則維護並實施管理服務提供商的政策和程序，以包括以下各項：	**12.8** 如果實體與服務提供商 (例如備份磁帶儲存設施、網路託管公司或安全服務提供商等託管服務提供商、或者接收資料用於分析欺詐模型的公司) 共用持卡人資料，則應透過觀察、審查政策和程序及審查支援文件，執行以下各項：			
12.8.1 維護服務提供商清單。	**12.8.1**確認服務提供商清單已得到維護。			
12.8.2 要求服務提供商出具書面合約，由其確認對自己擁有的持卡人資料的安全性負責，並保留此合約。	**12.8.2** 確認書面合約包括服務提供商確認其負責保護持卡人資料安全的責任。			
12.8.3 確保已建立雇用服務提供商的程序 (包括雇用前相應的盡職調查)。	**12.8.3** 確認這些政策和程序已記錄並得到遵守 (包括雇用任何服務提供商之前相應的盡職調查)。			
12.8.4 維護計劃，以每年至少監控一次服務提供商的 PCI DSS 遵從性狀態。	**12.8.4** 確認實體維護計劃，以每年至少監控一次服務提供商的 PCI DSS 遵從性狀態。			
12.9實施事故回應計劃。隨時準備立即回應系統漏洞事故。	**12.9** 獲取「事故回應計劃」和相關程序並進行檢查，執行以下各項：			
12.9.1 制訂事故回應計劃，以便在系統漏洞事故發生時實施。確保計劃至少可以處理以下各項： ▪ 出現威脅時的角色、責任以及溝通和聯絡策略，其中至少包括向支付品牌發出通知 ▪ 具體的事件回應程序 ▪ 業務恢復和持續程序 ▪ 資料備份程序 ▪ 分析法律要求，以報告出現的威脅 ▪ 涵蓋和回應所有關鍵系統元件 ▪ 參考或包括支付品牌的事件回應程序	**12.9.1.a** 確認「事故回應計劃」包括： ▪ 發生漏洞時的角色、職責和溝通策略，至少包括通知支付品牌： ▪ 具體的事件回應程序 ▪ 業務恢復和持續程序 ▪ 資料備份程序 ▪ 分析報告漏洞的法律要求 (例如，California Bill 1386 要求任何公司其資料庫中如有加州居民資料，在真正發現實際資料洩漏或懷疑資料洩漏時，必須通知受影響的消費者) ▪ 所有重要系統元件的範疇和回應 ▪ 參考或包括支付品牌的事件回應程序			
	12.9.1.b 審查有關以前報告的事故或警報的文件，確認記錄的事故回應計劃和程序得到妥善遵循。			
12.9.2 至少每年測試一次該計劃。	**12.9.2** 確認至少每年測試一次計劃。			

PCI DSS 要求	測試程序	到位	不到位	目標日期/備註
12.9.3 指定一天 24 小時、一週 7 天隨時準備回應警報的特定人員。	**12.9.3** 透過查看和審查政策，確認指定工作人員可執行一天 24 小時、一週 7 天的事故回應，並且監控範疇涵蓋任何未經授權的活動證明、未經授權的無線存取點的偵測、重要的 IDS 警報，和/或有關重要系統檔案或內容檔案未經授權變更的報告。			
12.9.4 針對負責回應安全漏洞的員工提供相應培訓。	**12.9.4** 透過觀察和審查政策，確認負責回應安全漏洞的員工定期接受培訓。			
12.9.5 包括來自於入侵偵測系統、入侵防禦系統和檔案完整性監控系統的警報。	**12.9.5** 透過觀察和審查政策，確認「事故回應計劃」涵蓋監控和回應來自於安全系統 (包括偵測到未經授權的無線存取點)的警報。			
12.9.6 根據以往的經驗教訓、結合行業發展情況制訂有關修改和改進事故回應計劃的程序。	**12.9.6** 透過觀察和審查政策，確認制訂根據以往的經驗教訓、結合行業發展情況修改和改進事故回應計劃的程序。			

附錄 A： 共同託管服務提供商的其他 PCI DSS 要求

要求 A.1：共用主機提供商必須保護持卡人資料環境

根據「要求 12.8」中的規定，所有可存取持卡人資料的服務提供商 (包括共用主機提供商)必須遵守 PCI DSS。此外，要求 2.4 還規定，共同託管服務提供商必須保護各實體的託管環境與資料。因此，共用主機提供商另外還必須遵守附錄中的要求。

執行評估：	測試程序	到位	不到位	目標日期/備註
A.1 根據 A.1.1 至 A.1.4，保護每個實體 (即商戶、服務提供商或其他實體)的託管環境和資料： 託管提供商必須滿足這些要求以及 PCI DSS 其他所有相關部分的要求。 ***註：*** *即使託管提供商可以滿足這些要求，也不能保證託管服務提供商所服務的實體的合規性。各實體必須 符合 PCI DSS 規定並驗證合規性 (如適用)。*	**A.1** 尤其是對共用托管提供商進行 PCI DSS 評估時，如要確認共用托管提供商保護實體 (商戶和服務提供商)的託管環境和資料，請從託管商戶和服務提供商的代表性樣品中抽樣選擇伺服器 (Microsoft Windows 和 Unix/Linux)，並執行以下從 A.1.1 至 A.1.4 中的內容：			
A.1.1 確保每個實體僅執行可存取該實體持卡人資料環境的程序。	**A.1.1** 如果共用托管提供商允許實體 (例如商戶或服務提供商)執行他們自己的應用程式，請確認使用這些實體唯一的 ID 執行此類應用程式的程序。例如： 系統中的任何機構都不得使用共用的網路伺服器使用者 ID。 機構使用的所有 CGI 指令碼在建立和執行時都必須作為該機構唯一的使用者 ID。			
A.1.2 僅限每個實體在自己的持卡人資料環境內存取。	**A.1.2.a** 確認任何應用程式程序的使用者 ID 不是有權限的使用者 (根權限/管理員權限)。			
	A.1.2.b 確認每個實體 (商戶、服務提供商)擁有的讀取、寫入或執行權限僅可用於其所屬檔案或目錄或者必要的系統檔案 (透過檔案系統權限、存取控制清單、chroot、jailshell 等加以限制) **注意：** 機構的檔案不能與群組共用。			
	A.1.2.c 確認實體使用者對共用系統二進位檔案沒有寫入權限。			

執行評估：	測試程序	到位	不到位	目標日期/備註
	A.1.2.d 確認只有擁有日誌項目的實體才可檢視其項目。			
	A.1.2.e 為確保每個實體不會獨佔控制伺服器資源繼而利用漏洞 (例如，錯誤、race 和重新啟動會導致像緩衝區溢出這樣的情況)，請確認已針對系統資源的使用情況部署了相關限制： ▪ 磁碟空間 ▪ 頻寬 ▪ 記憶體 ▪ CPU			
A.1.3 確保已啟用日誌和稽核記錄，它們對每個實體的持卡人資料環境都是唯一的，而且符合 PCI DSS 要求 10。	**A.1.3** 確認共用托管提供商已針對每個商戶和服務提供商啟用日誌記錄，具體如下： 已針對第三方一般應用程式啟用日誌。 日誌在預設情況下處於活躍狀態。 只有擁有日誌的機構才能查看其日誌。 日誌位置已明確通知給擁有它的機構。			
A.1.4 啟用在任何託管商戶或服務提供商出現漏洞時及時提供取證調查的程序。	**A.1.4** 確認共用托管提供商制訂的書面政策包括在發現漏洞時提供相關伺服器的及時取證調查程序。			

附錄 B： 補償性控制

當實體由於合法的技術限制或記錄的業務限制無法滿足
明確陳述的要求，但已透過實施其他措施或補償性控制充分減輕了與此類要求相關的風險時，對於大多數 PCI DSS 要求可以需要考慮採用補償性控制。

補償性控制必須滿足以下標準：

1. 符合原始 PCI DSS 要求的目的和嚴格程度。
2. 提供與原始 PCI DSS 要求相似的防護水平，以便補償性控制能夠充分防範原始 PCI DSS 要求所要規避的風險。(請參閱《*導覽 PCI DSS*》，瞭解各項 PCI DSS 要求的目的。)
3. 「超越」其他 PCI DSS 要求。(如果只是遵從其他 PCI DSS 要求，則不是補償性控制。)

   評估補償性控制是否「超越」其他 PCI DSS 要求時，請考量以下內容：

註： *以下 a) 到 c) 項只是範例，所有補償性控制的充分性必須由執行 PCI DSS 審查的評估機構進行審查和驗證。補償性控制的有效性取決於實施控制的具體環境、週邊的安全控制以及控制的設定。公司應該知曉，特定的補償性控制不是在所有環境中均有效。*

a) 如果現有的 PCI DSS 要求已在接受審查的項目要求範疇內，則不得視為補償性控制。例如，在發送非主控台管理存取密碼時必須加密，以降低純文字管理密碼遭到攔截的風險。如果密碼沒有加密，實體不能使用其他 PCI DSS 密碼要求 (入侵者鎖定、複雜密碼等) 對此進行補償，因為這些密碼要求不會降低純文字密碼遭到攔截的風險。而且，其他密碼控制也已在接受審查的項目 (密碼) 的 PCI DSS 要求範疇內。

b) 如果現有的 PCI DSS 要求是其他領域所要求的，但不在接受審查的項目要求範疇內，則可以視為補償性控制。例如，雙因素驗證是一項針對遠端存取的 PCI DSS 要求。當系統無法支援傳輸加密的密碼時，也可將*內部網路內*的雙因素驗證視為針對非主控台管理存取的補償性控制。如果雙因素驗證滿足以下條件，則可視為可接受的補償性控制：(1) 透過減少純文字管理密碼遭攔截的風險，達到最初目的的要求；(2) 經適當設定且在安全的環境中執行。

c) 現有的 PCI DSS 要求可與新的控制結合成為補償性控制。例如，如果公司無法按照要求 3.4 使持卡人資料具有不可讀性 (例如，透過加密方式)，則可利用解決以下所有問題所需的裝置或包括裝置、應用程式和控制件的組合構成補償性控制：(1) 內部網路區段劃分；(2) IP 位址或 MAC 位址過濾；及 (3) 內部網路內的雙因素驗證。

4. 與不遵循 PCI DSS 要求而引發的其他風險相對應

評估機構應按照上述 1-4 項，在每年的 PCI DSS 評估中，對補償性控制進行徹底評估，以驗證各補償性控制能否充分應對原始 PCI DSS 要求所要規避的風險。為了保持合規性，必須制定程序和控制措施，以確保補償性控制在評估完成後仍然有效。

附錄 C： 補償性控制工作表

使用補償性控制以滿足 PCI DSS 要求時，請使用此工作表針對任何要求定義補償性控制。注意，補償性控制也應在相應 PCI DSS 要求部分的《遵從性報告》中予以記錄。

註：
只有已接受風險分析且有合法的技術限制或明文規定的業務限制的公司，才可以考量利用補償性控制來實現合規。

要求編號和定義：

	所需資訊	解釋
1. 限制	列出妨礙達到原始要求的限制。	
2. 目標	定義原始控制的目標；識別透過補償性控制達到的目標。	
3. 識別的風險	識別由於缺少原始控制而引起的任何其他風險。	
4. 補償性控制的定義	定義補償性控制，並解釋其如何達到原始控制的目標及應對增加的風險(如果有)。	
5. 補償性控制的驗證	定義如何對補償性控制進行驗證和測試。	
6. 維護	定義為維護補償性控制而制定的程序和控制措施。	

補償性控制工作表 – 完成的範例

對於任何透過補償性控制標注為「到位」的要求，請使用此工作表定義補償性控制。

要求編號： *8.1—*

在允許所有使用者存取系統元件或持卡人資料之前，是否透過唯一的使用者名稱對其進行識別？

	所需資訊	解釋
1. 限制	列出妨礙達到原始要求的限制。	*公司 XYZ 使用了沒有 LDAP 的獨立 Unix 伺服器。因此，每個人都需要「根」登入，但公司 XYZ 不可能管理「根」登入，也不可能記錄每位使用者的所有「根」活動。*
2. 目標	定義原始控制的目標；識別透過補償性控制達到的目標。	*要求使用唯一登入的目標有兩個。首先，從安全角度來看，共用登入認證是不可接受的。其次，如果使用共用的登入，則無法明確指明要對某個特定動作負責的人是誰。*
3. 識別的風險	識別由於缺少原始控制而引起的任何其他風險。	*由於不能確保所有使用者都有唯一 ID，因此無法對使用者進行追蹤，這樣便會使存取控制系統面臨更多風險。*
4. 補償性控制的定義	定義補償性控制，並解釋其如何達到原始控制的目標及應對增加的風險 (如果有)。	*公司 XYZ 將要求所有使用者使用 SU 指令，從各自的桌面登入伺服器。SU 不但可以讓使用者存取「根」帳戶並在「根」帳戶下執行動作，還可以在 SU 記錄目錄中記錄使用者的動作。這樣，便可透過 SU 帳戶來追蹤每個使用者的動作。*
5. 補償性控制的驗證	定義如何對補償性控制進行驗證和測試。	*公司 XYZ 向評估機構證明，SU 指令已在執行，且已記錄利用該指令的個人，以識別此人在根權限下執行動作。*
6. 維護	定義為維護補償性控制而制定的程序和控制措施。	*公司 XYZ 記錄了相關流程和程序，以確保不會發生以下情況：個別使用者為了在執行根指令時逃避追蹤或記錄而變更、修改或移除 SU 設定。*

附錄 D： 商業場所/系統元件區段劃分與抽樣