百煉鋼化繞指柔

PCI DSS 產品經理 Gina Kuo 專訪

郭巧君（Gina Kuo）|
BSI 台灣 PCI DSS 支付卡產業資料安全標準產品經理

責任編輯 徐瑋琳　採訪撰文 鄭詠中　校正修訂 黃純郁

PCI DSS（Payment Card Industry Data Security Standard）支付卡產業資料安全標準，是五大國際支付卡品牌[1]為支付卡產業保障持卡人資料安全所共同建置的統一規範[2]。所有從事持卡人資料之保管、處理、傳輸的機構，均須關注其組織是否符合 PCI DSS。

本次BSI台灣電子報很榮幸邀請PCI DSS支付卡產業資料安全標準產品經理Gina Kuo。由 Gina 親自介紹 PCI DSS 的概念內涵，對應到刷卡授權的運作連結，以及如何達到保護持卡人資料安全；持卡人日常發生的支付動作，涉及個人金融資訊安全的保護如何啟動，於文中得知究竟。而 Gina 結合金融與資安兩大趨勢的專業背景，在擔任稽核員與講師現場，務實體貼耐性換位思考、百鍊鋼化繞指柔，洗鍊精彩。且聽 Gina 娓娓道來，細細分享。

溫柔堅定專業底 熬過轉換期

Gina 大學與研究所主修都是資訊管理，進入 BSI 之前在勤業眾信聯合會計師事務所多年擔任電腦審計，進入 BSI 台灣負責資訊安全風險管理稽核工作。從電腦輔助稽核技術（CAATs），到資訊系統安全控制、企業內部控制措施設計與評估，都累積豐厚的經歷。


Gina 去金門稽核，客戶熱情地替她攝影留下紀念。

問到過去從事電腦審計稽核到現在資安標準系統稽核的差異，Gina 從稽核範圍、對應層級和執行內涵說明：從事電腦審計稽核，只針對客戶的財報系統安全做確認，主要面對的窗口就是該客戶的資訊部門，查核準則是由事務所制定的制式規範。擔任 BSI 稽核員，替客戶稽核的範圍有可能擴及整個公司，大部分面對的會是高階主管；同樣的標準架構

1 VISA、MasterCard、JCB、AMEX 與 Discover，所成立的 PCI SSC 支付卡產業安全標準協會。
2 為保障持卡人的資料安全，繼而針對安全管理、政策、程序與方式、網路配置與軟體設計等多方需求，所訂定之資料安全標準。

套在不同單位組織、會長出屬於自己文化內涵，稽核員依此就相關流程是否符合 ISO 精神去做查證。雖然兩項工作都是以資訊安全管理知識為基底，但前後對照之下工作差異仍然存在。Gina 坦言剛轉換到 ISO 查核是有陣痛期，**ISO 稽核是一個大量溝通的過程，稽核員除了具備標準知識，與人應對溝通的技能也同等重要。前者可以跟著 Mentor 學習、靠努力快速累積，後者需要一次次靠經驗建立出具有個人特質的溝通能力，無法短時間可以達成。**來到 BSI，Gina 認為學習最多的，就是與客戶高層人員的對應，以及面對更廣的稽核範圍，要如何溝通執行。

即使說起過往當下的困難，Gina 始終語氣溫和。想必當初也是持著這般溫柔堅定，本著專業基底，熬過了轉換跑道的陣痛期。

PCI DSS 規範對象與運作

來談讀者感興趣的 PCI DSS 支付卡產業資料安全標準。Gina 先與大家說明：PCI DSS（Payment Card Industry Data Security Standard）是由 PCISSC 支付卡產業安全標準協會（見上頁註腳 1），針對支付卡資料安全制訂的標準，支付卡的資料主要包括：卡號、有效年月以及末三碼（安全碼）、磁條資料等，主要目的是保護這些卡片資料預防被盜刷。PCISSC 委員會成立之前，各家支付卡品牌有各自的安全標準，提供刷卡服務的商家必須要了解各家的安全標準並遵循。2006 年起委員會成立並制定各項統一標準之後，商家只需遵循 PCI DSS 即可同時符合五家支付品牌的資料安全標準。

支付卡產業中參與的每個角色，都需要遵循 PCI DSS 規範以確保支付卡資料之安全。相關角色包含：發卡機構、收單機構、商家（實際提供產品與服務單位），以及服務提供者[3]。其中 PCI DSS 規範商家及服務提供者須透過自評表或是第三方驗證確認遵循程度[4]。

PCI DSS 與 ISO 27001 的架構和要求相似，但最大的差異在於 PCI DSS 的每項要求都更為明確及嚴謹，例如針對通行碼（password）強度要求，PCI DSS 要求最少要 7 碼、英數字混和、90 天變更、不可與前 4 代重複等。因此**對一般企業或組織來說，不管有沒有牽涉到支付卡業務，都很推薦參考 PCI DSS 作為資訊安全的實作指引。**

針對 PCI DSS 的第三方驗證，必須由 PCI SSC 認可的 QSA（Qualified Security Assessors）──合格的安全評估商執行，而 BSI 就是屬於合格的安全評估商，目前針對 PCI DSS 提供過服務的客戶產業包括實體商家、網路購物商家、航空業線上購票、支付 APP、IDC 機房等。Gina 說要通過 PCI DSS 稽核驗證，當然會有對應的成本，但也真的能讓組織

[3] 提供支付卡服務，如：行動支付業者；或是提供會影響支付卡交易安全之服務，如：雲端平台業者。

[4] 此部分由各家支付品牌決定，例如 VISA、MASTERCARD、JCB 是由刷卡交易量決定商家或服務提供者要填寫自評表或是要由第三方驗證。

加強資訊安全相關控制。另一個附加價值是，**當今國人資安意識提高，對支付卡使用安全敏感度也日漸注重，Gina 提到像是生活中搭乘計程車使用車隊的 APP 綁訂支付卡支付時，或是在線上電商購物平台購物時，若有標示通過 PCI DSS 驗證，也會讓消費者較安心進行支付卡消費。**

換位思考 柔化張力

Gina 的工作也負責大量客戶資訊安全稽核，Gina 說，每個被稽核的單位，大都不希望被稽核員提出缺失，這是人之常情，因此在討論稽核發現時難免會遇到需要大量溝通協調的時候。Gina 都能盡量站在對方的立場以及風險點討論：「提出任何缺失，**都會先確認提出這個項目對客戶是否有幫助？實際的風險在哪裏？**」另外當遇到還有疑慮的客戶時，Gina 會告訴客戶：「稽核主要是要確認你們符合要求的證據，而不是來找不符合的證據。」基於事實的善意提醒，讓客戶回到稽核的本質與初衷。

每次訪 BSI 產品經理，一定要問對稽核與教育訓練工作的心得。Gina 說稽核和擔任講師共同之處，就是都要講非常多的話。稽核現場，要問問題、覆述客戶的敘述、溝通稽核結論；不過相比之下，訓練課程講的話量更多。另外稽核現場遇到的客戶，通常本身已有資訊相關背景知識，而訓練課程的學員背景有時會相當多元，因此在講解上要更加淺顯易懂。「**溝通和表達能力對稽核員與講師都很重要，因為都要讓對方聽得懂你在講什麼**」Gina 曾告訴稽核員訓練課程的學員：「至於稽核員的溝通風格無論是親切或嚴格，都屬個人特質，沒有對錯高低，**最大的目的都是要讓稽核順利完成。**」

Gina 在 BSI 台灣辦公室留影，整個人的氣質和環境就是這麼融合，散發「不著痕跡收服人心」的魅力。(攝影：黃純郁)

親切的日常

還是忍不住問及 Gina 都如何處理稽核工作壓力？Gina 的回答是：網購與追劇。Gina 在網購上相當精於比價，能夠在同樣的品質以最低的價格購得，十分有成就感。稽核員每日工作包含大量的移動往返，交通過程中 Gina 也看劇，類型多樣不受限，還可以和念小學的女兒一起交換看劇心得，彼此推薦。知道 Gina 的紓壓興趣，怎麼就讓人理所當然地放心了呢，稽核員也愛網購和追劇，人生不用時時刻刻奮進。

如 BSI 風險行銷專員、也是本專訪的校訂編輯 Tracy Huang，對這次採訪 Gina 的感言：「感受到不著痕跡收服人心的魅力。」整篇文章讀下來，從稽核教學現場到藏於生活中的關鍵冷知識，收穫豐富又不會感到壓力。身懷稽核專業又待人十分親切，這是屬於 Gina 的獨特魅力。- 全文完 –

BSI Careers

- 更多 BSI 稽核老師的專訪內容請前往 BSI 官網閱讀
- 聯絡 BSI：infotaiwan@bsigroup.com | 02-26560333