強大而輕盈

BSI 資深稽核員 Emily Wen 專訪

溫雅珊（Emily Wen）|
BSI 台灣驗證部副協理暨 ISO 27001 產品經理

責任編輯 徐瑋琳　採訪撰文 鄭詠中

今年三月，Emily 榮升驗證部網路安全及資訊韌性副協理（Assistant Director CSIR - Cyber Security & Information Resilience）。身為風險系列標準資深稽核員與 ISO 27001 產品經理，在這萬物皆連網、全球資安意識大爆發時代，Emily 擔任 BSI 台灣驗證部管理職更是別具意義。BSI 電子報特別邀請 Emily 接受專訪，從她的個人經驗與特質，理解資深風險稽核員養成之路、身為驗證部門管理者如何落實人才培育與運用，以及從市場面分析未來趨勢。即使行程忙碌，Emily 受訪前仍細細消化採訪大綱，將題目融會貫通盤整回覆，相當厚實精彩的專文，編輯小組深感學習良多，誠摯與電子報讀者分享。

》》 邏輯清晰 耐心理解的理科女生

Emily 於 2006 年進入 BSI，國人業界對於資安還處在「出事再說」的上古年代。現任 BSI 東北亞區總經理蒲樹盛（Peter）當時面試 Emily 後，就決定邀請她加入 BSI。「Peter 有說選擇我一方面的原因是，我是女生。他在跟我談話的過程當中，感覺到我特別細心有耐性」過往內幕可以大方說出來了，Emily 多年來優秀的表現與今日的擔當，沒有人會認為是稽核業內少數性別特權所致。也說自己從小就是數理方面成績表現優異，邏輯、排列組合和微積分特別好，與身俱來的好能力，到現在都支持著 Emily 往前推進：「後來發現邏輯好真的很重要—尤其接下部門主管後，當許多事情湧進來，邏輯清楚就知道先後順序。」上任之後，Emily 自訂的首要任務：一個是「人才的培育與運用」，一個是「標準與市場的連結開拓」。很開心聽到 Emily 說上任至今，事情都有如預期一一落實在軌道上，Emily 說關鍵是要有很大的信念。我們也替大家紀錄彙整 Emily 這兩大區塊的方向與運行脈絡。

》》 人才培育與運用秘笈

人才鑑別與善用

大家都以為以資安風險為專業的稽核員都有類似的專業背景和個人特質嗎？Emily 說，就像風險標準分為：條款寫得很仔細的網路安全屬性標準，以及標準內容精簡、但需要明確界定出範圍與何謂做得好的資訊韌性型標準—前者需要細心精確按表核實，後者需要良好的邏輯與溝通能力—稽核員也是同理。當上主管之後，Emily 更是會從同仁的優點和潛能切入，做好人才鑑別，安排人力與不同的部門與專案合作，讓個人長處得以發揮，而非用一套標準套在個人身上去審視優劣。

稽核員養成之路

BSI 可以提供給客戶的服務中，稽核和訓練課程是主要的兩塊。BSI 的講師向來赫赫有名，很知道如何把標準知識傳遞到學員手上。「但是不是所有的稽核員都能當講師」Emily 坦白說：當講師這個工作，除了努力學習，個人特質要佔的比例更多，不過，講師的經驗對稽核絕對有大大的幫助：「在當講師的過程，你會碰到各式各樣的學員，提出千奇百怪的問題」**能當 BSI 的講師，對標準內容和流程就是要異於常人的清楚。**

這是 Emily 工作的神情，即使工作壓力再大，事情再多，她總是能有條不紊地把事情按優先順序一一處理。

Emily 提起比自己更早進入到 BSI 的資深稽核員，像是 Benson、Steven 這幾位品質管理系統課程的名師，以前看他們在稽核時藉由和現場的客戶對談聊天，就能抓出客戶在系統流程上的問題出在哪裡，這功力是多年稽核加課程百煉千錘後的累積。**Emily 說自己現在看稽核缺失也是從更大的高度去替客戶找到原則性的問題，客戶亦是感謝也感到安心。**

》》 標準與市場的連結開拓

時至今日，包含電信與金融這些龍頭級產業等大型企業，拿到 ISO 27001 資訊安全管理系統驗證是普遍的基礎。從需求切入，看各風險標準系統與市場連結與待開拓領域，以下是 Emily 的說明分析：

因法令法規要求

2019 年資通安全法上路，在法令要求之下，政府單位、非政府單位但屬基礎建設，或替政府單位承接相關業務者，以及屬金管會管轄的保經保代金融保險單位，會是這一波受法定要求之下，將 ISO 27001 資訊安全管理系統、PIMS 個資管理系統[1]以及 ISO/IEC 20000 服務管理系統，逐步納入進行標準導入與驗證。

做深做廣 績效彰顯

已有 ISO 27001 資安基礎的企業單位，Emily 會爲其從上到下檢視，依其組織需求在 PIMS 個資管理與營運持續管理做建議。而像是 ISO 27017、ISO 27018 雲端個人隱私保護標準則是看業務屬性，並不一定適合每一個客戶。Emily 不強調標準要拿得多，同樣 ISO 27001 很多企業單位過去稽核範圍在資訊單位，鼓勵可將業務與行政單位納入，畢竟組織的營運與業務推廣都有賴資訊系統支持。有鑑於此，原本資訊單位更需要透過營運持續管理系統以彰顯績效──大家都知道，IT 部門表現向來難以計算，被注意到時往往就是

[1] 個資管理系統（PIMS）包含各項隨時間需求頒布的國際標準：ISO/IEC 27701 與 ISO/IEC 27001、BS 10012、ISO/IEC 29100、ISO/IEC 29151、ISO/IEC 27018 或其他國際標準可相輔相成。無論是面臨本國個資法、歐盟 GDPR 又或是國際間的各項個資管理規範或要求，確實掌握國際標準間的要點並正確運用，讓個資管理系統（PIMS）落實的更加完善，將是遵循法規並增強外部信賴的關鍵，有效因應最新管理議題，持續實踐永續經營。Emily 於採訪中在在提到：同一個標準對不同企業有不同意義，而該如何選擇哪些 PIMS 標準，歡迎與我們聯繫取得建議：https://www.bsigroup.com/zh-TW/12/general-enquiry/

出問題了。ISO 22301 / BCM 營運持續管理系統，倘若天災或人為事件（地震或遊行都是台灣有機會遇到的情景），資訊單位與企業組織該如何服務不中斷展現韌性？國內代表性大廠日月光與聯電，都在今年以取得 BSI 營運持續管理驗證通過為目標。

回顧與前瞻 藉稽核建立優秀的習慣

Emily 說起剛進 BSI 推行 BS 7799，怎麼推或者台灣的市場需求到底在哪裡，其實是模糊的。在 BSI 與顧問、客戶三方共同摸索討論之下，開始有了清楚的形貌。**每一個國際標準並非引進之後就可順利推行，落地化過程總是點滴成型才能真正符合當地所需。**BSI 台灣 BCM 產品經理暨資深稽核員 Wayne Yang 為國際營運持續組織 BCI（Business Continue Institution）全球會員[2]，BCI 每年會向會員提出影響營運持續十大威脅統計報告[3]，其中 IoT 排名逐年上升，監視器、家庭網路與資訊安全都有聯結，免費 App 背後可能是間諜軟體，資訊安全已與生活連結。

強大而輕盈

面對日日壓力，Emily 仍能保持清晰並游刃有餘。利用週末到鄉間與父親相聚、和土狗玩、吃鄰里自種蔬果，夜間走到戶外一抬頭就能看見滿天繁星。還有每年都會進行一到兩次大旅行，至今 Emily 已到過五十個國家探尋（不代表只出國五十次、像是日本就去超過十次），其中包括一般國人較少前去的地區。無論週末暫離台北，或年度大旅行，都是 Emily 給自己的重開機（Reset）儀式。

採訪當日 Emily 按個人品味穿搭出席，採訪完畢應要求，坐在咖啡館戶外區拍照，自然如網美街拍。上一次 BSI 電子報訪問 Emily 是 2007 年秋，多年來美麗智慧如昔。越認識越讓人驚奇的 Emily，用輕盈面對層層挑戰，以身示範：強大可以如此輕盈。- 全文完 -

今年五月 Emily 的以色列之旅，騎著毛驢上山看神殿。神殿之路後段只能步行，那天 Emily 走了 21.7 公里。

BSI Careers

- 閱讀〈強大而輕盈─BSI 資深稽核員 Emily 專訪〉完整版請點此
- 聯絡 BSI：infotaiwan@bsigroup.com | 02-26560333

[2] 會員資格需考試通過方能取得。

[3] BSI 連年與 BCI 組織合作發布地平線掃描報告(Horizon Scan report)，報告中呈現出受訪者對長短期營運威脅的預期及受影響的結果，已經成為專業人士進行風險和威脅評估的重要參考資源。BSI 於每年終舉行資安風險年會，剖析此報告內的重要資訊，協助與會來賓規劃來年的營運持續的情境演練和計畫。點此報名 2019 資安風險年會>