用標準找到資通安全管理法的落實路徑

NIST 網路安全框架 / COBIT / NIST SP 800-53 / BS 31111 網路風險與韌性

受訪：BSI 英國標準協會客戶經理
孫文良（Sunny Sun）▶

撰文整理：鄭詠中
校閱修訂：孫文良

從今年一月一日《資通安全管理法》上路以來，坊間各式各樣關於法條的解釋論述以及證照需求課程紛紛出籠。鑑於立法目的為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益且資訊科技發展成為國家整體競爭力的象徵，BSI 身為國際標準制定者與資安推動者，樂見資安能量大爆發，立法初衷風行草偃。

資安法制定過程參考大量國際資安標準內容。標準是眾人智慧且經過驗證之結晶。本篇專文，提供及整理不同標準之特色與切入角度，**由於考量多數組織已建立資訊安全管理系統 ISO 27001（ISMS），常見組織以 ISMS 為主體進行與資通安全管理法要求的差距分析，而為了符合法規要求的完整性，BSI 選擇利用其他標準與框架的核心優點，補足在主體上的不足。**而在標準選擇的方向上，主要以能夠對組織產生最大價值、提升組織韌性與隱私保護的面向進行考量，由上而下、由內而外的方式組成，整合了 NIST、COBIT 與 BS 31111 等國際標準框架，因組織之資訊系統已成為組織營運不可或缺的一環，常在控制、成本與營運持續等面向進行考量。

深入比對法條內涵與執行項目，提供更全面完善的法論概念與落實路徑，並使用以下六大面向帶出《資通安全管理法》核心重點：

- 主管機關權責
- 委外管理
- 資通安全維護計畫
- 資通安全事件通報
- 資通安全情資分享
- 資通安全管理監督稽核與持續改善

考量行政院在制定資通安全管理法其法律結構，主要以主管機關應辦事項、公務/非機關資通安全管理、目的與罰則五個面向，轉對應到實務之資訊安全管理，若**改以此六個面向的角度來進行相關法規遵循的執行，更容易直接整合進組織原來已熟悉且持續運作的資訊安全管理系統中。**例如：資通安全維護計畫即可對應到組織建立的資訊安全政

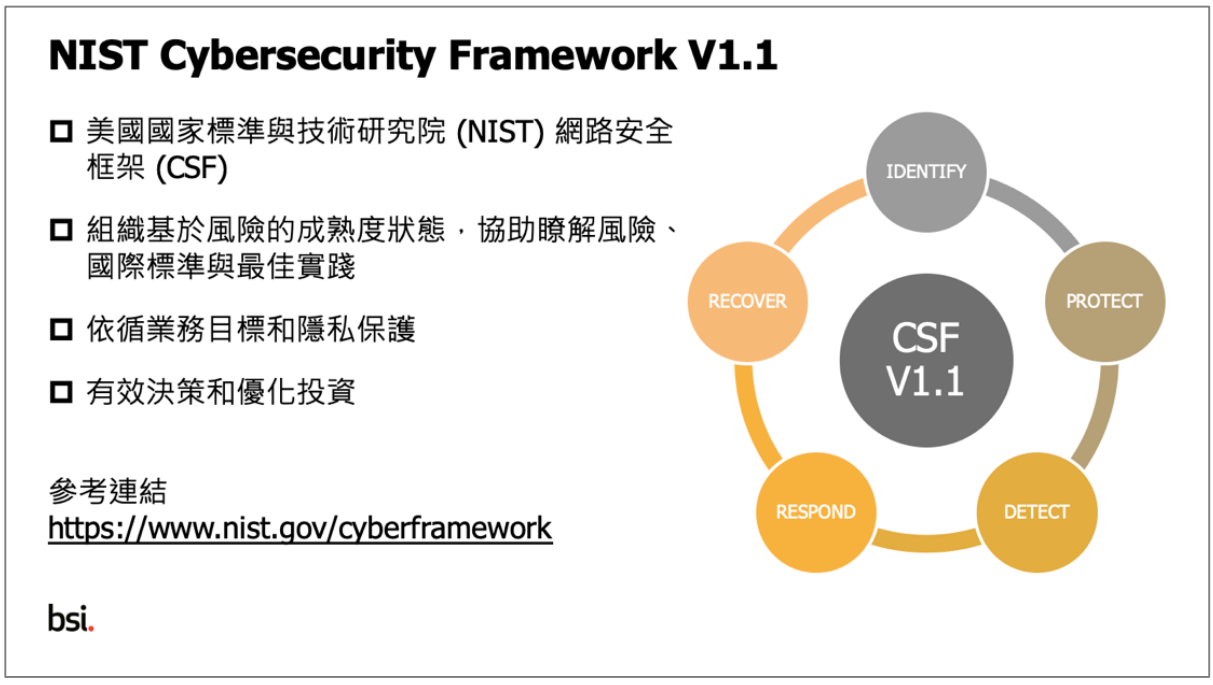
策。因此無論是公務機關、非公務機關，容易掌握各自的權責、要盡到的義務與責任、監督與稽核等必須要做的事情，以及做為後續實作的依據。

四大標準的採用與落實

在此並提出四個國際常用資安標準框架：NIST Cybersecurity Framework V1.1、COBIT 5、NIST SP 800-53 Revision 4 和 BS 31111:2018 Cyber risk and resilience。各標準介紹與挑選出對應落實案例擬列如下：

NIST Cybersecurity Framework V1.1

來自美國國家標準與技術研究院的網路安全框架，簡稱 NIST CSF。針對關鍵基礎設施風險設定，並有去思考是否能適用所有的產業，因此在制訂框架時有將上述因素都考量進去。此框架分五個主軸：識別/保護/偵測/回應/回復 (和 PDCA 很像)，很符合我們時常在做的事故管理、事故回應。此標準就是把 Cybersecurity 的框架做到與組織目標緊密的環節裡面：針對你的現況，跟你未來預期想要達到的目標做比較，又涵蓋了隱私保護進去 (現在的資訊安全議題中，個資和隱私保護是近年來的重點，也和商譽有直接的風險連結)。此外，它包含優化的決策，就是做什麼事情能讓您效益最大。比如說，您現在有些目標只做到 60 分，有的做到 80 分。那是否可以花一點點錢，讓 60 分到 80 分。這和服務水準協定 (SLA) 中的妥善率邏輯是一樣的，這個框架也會引導到這部分。



〈圖一〉NIST CSF 標準架構與特色

落實案例：

一、「主管機關權責」中的委外管理

NIST CSF ID.SC-3：與供應商和第三方合作夥伴簽訂合約，目的在實現組織網路安全計劃和網路供應鏈風險管理計劃目標的適當措施。

強調供應商與第三方合作夥伴的簽約，涵蓋到風險管理目標，就不只是和對方簽個約而已──相信大家跟廠商合作，除了在採購期間有維護合約的保固，要思考的是：三年保固期過後，您是否還繼續會買保固？這牽扯到大筆的預算，以及若是不做，遇到真正的安全風險時是否會有問題。此外，廠商的監督該如何進行？若實際去廠商端做二者稽核，也會面臨到非自身領域和熟悉的專業問題。會身負二者稽核的不外乎是組織裡的內稽人員，有的甚至會帶專業的 IT 夥伴，做專業知識協助，這樣對供應鏈的稽核深度才夠。若只有單一稽核人員去看，強度是不夠的。

二、「委外管理」中的資通訊系統或委外服務管理

NIST CSF ID.SC-2：使用網路供應鏈風險評估流程識別，確定優先級並評估資訊系統，組件和服務的供應商和第三方合作夥伴。

NIST CSF ID.SC-3：與供應商和第三方合作夥伴簽訂的合約用於落實組織網路安全計劃和網路供應鏈風險管理計劃目標的適當措施。

NIST CSF ID.SC-4：供應商和第三方合作夥伴透過稽核、測試結果或其他形式的評估進行例行評估，以確認他們是否履行了合約義務。

NIST CSF PR.AT-1：所有用戶都被告知並接受過訓練。

記得評估流程確定優先層級。與第三方的合作關係和網路供應鏈的管理計畫目標，要有適當的措施。**第三方合作夥伴要通過稽核，稽核可以自己做，不見得要委外，重點是要確定對方是否有履行合約。所有任務都要告知並接受訓練，不一定是要上課，但一定要把你的資安要求講清楚，不然供應商要如何知道怎麼符合要求？**

三、「資通安全事件通報」

NIST CSF RS.RP-1：回應計劃在事件發生期間或發生之後執行

NIST CSF RS.CO-2：報告的事件符合既定標準

NIST CSF RS.AN-2：了解事件的影響

NIST CSF RS.MI-1：事件被遏制

NIST CSF RS.MI-2：減輕事故的發生

NIST CSF RS.IM-1：回應計劃包含經驗教訓

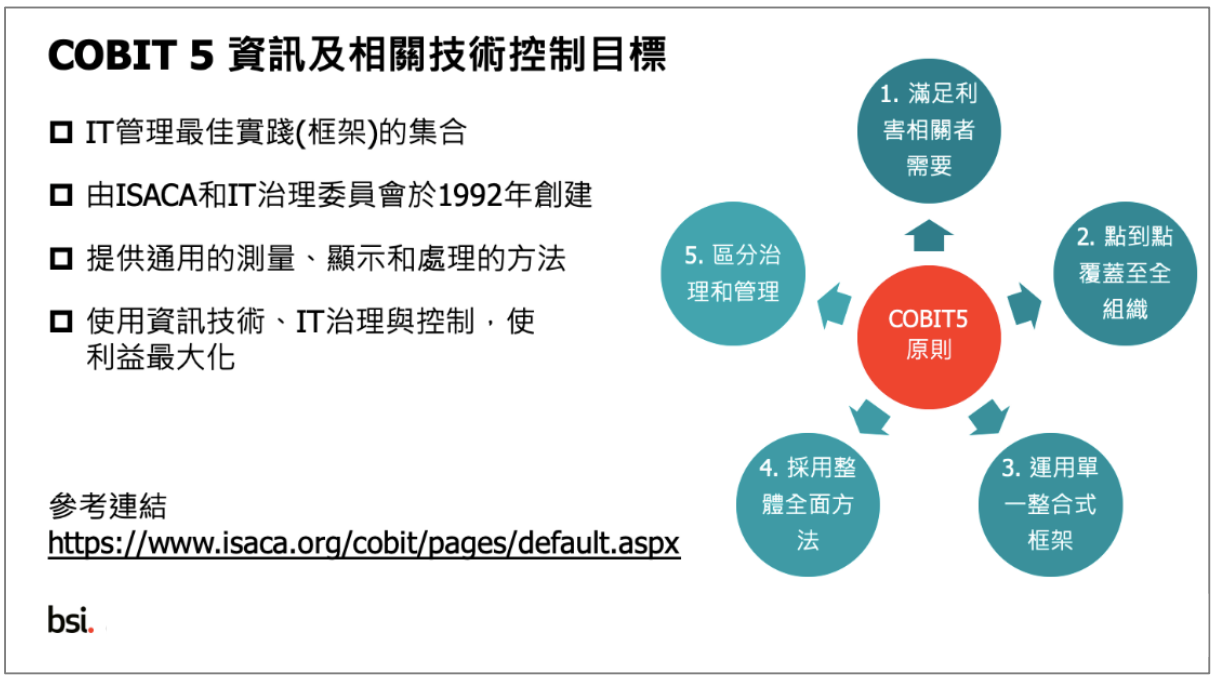
NIST CSF RS.IM-2：更新回應策略

NIST CSF RC.RP-1：在遭遇網路安全事件期間或之後執行復原計劃

事件發生或之後的回應計畫，若不能適用，可能還要更新回應策略。所有相關事件都要在回覆後做處理，減輕事故發生。建議可參考 NIST CSF 這樣的標準，看自己之後有哪些可以施行的項目。

COBIT 5

雖然它現在最新版本已經出到 2019，但目前最成熟的是在第 5 版，應用的人也比較多，建議各位以第 5 版做參考，從中引用。COBIT 做控制目標，有五大原則：第一個真的有考慮到利害關係人。第二個就是端到端、點到點。第三個是做到整個組織是貫穿的架構。第四個是整個架構採取全面方法。第五點是區分治理和管理。管理和治理，越來越分開來談了，不是做好資訊安全就可以，可能是要將資訊安全帶進整個企業的管理治理框架，讓我們的運作可以從頭到腳。你一定要把你的 Security 和 IT 的投資反映到整個企業的營運目標上，不然我們為什麼要做？



〈圖二〉COBIT 5 標準架構與特色

落實案例：

一、「資通安全維護計畫」中的資通安全政策與目標

COBIT 5 APO01.03 維持管理系統的促成者

COBIT 5 APO02.01 了解企業方向

COBIT 5 APO02.06 溝通 IT 戰略和方向

COBIT 5 APO03.01 發展企業架構願景

COBIT 5 APO13.01 建立並維護資訊安全管理系統（ISMS）

我們都知道整個資安的運作是 Top 到 Down 的而不是 Bottom up 上去，請先思考誰是維持管理系統的促成者。要瞭解企業方向，IT 戰略和方向也一定要和企業方向一致，並得以發展企業架構願景。標準建議要建 ISMS，不見得一定是 ISO 27001，你要建一個自己的 ISMS 也可以，只是 ISO 27001 是大家行之有年的框架，運用上來講是比較熟悉，也比較沒有問題的。**你可以建立自己的制度，有一個運作完善的 PDCA 循環，相信在資通安全管理法的符合性就可以拉得很高，包含委外單位的適任性。**

二、「資通安全維護計畫」中的資通安全防護及控制措施

COBIT 5 APO11.04 執行品量監控，控制和審查

COBIT 5 BAI06.01 評估確定優先級並授權變更請求

要先定義，根據定義，持續監控流程和服務的品質。然後按定義施行測量。評估優先等級與授權變更申請：**請記得把 IT 和業務考量進來。為何系統更新都發生在深夜？因為考量到把對業務的影響降到最低。**評估變更是否會對營運環境產生負面影響，並引入不可接受的風險？然後，確保記錄、優先級、分類、評估、授權、計劃和計劃更改：一定要做好記錄，出了事才回頭看，原來昨天有做變更──這樣的情況在很多組織都發生過，很不可思議，但就是發生了。

三、「資通安全情資分享」評估與因應

COBIT 5 APO12.06 回應風險

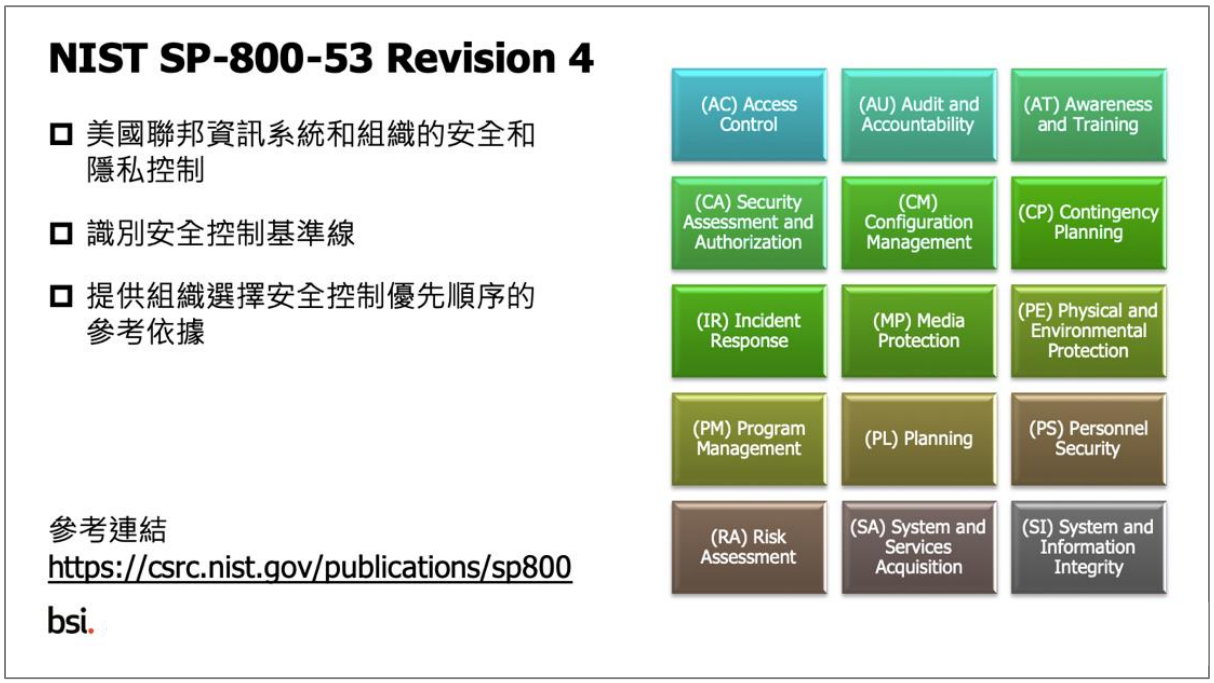
COBIT 5 BAI08.04 使用和分享知識

風險回應：發生事件時，要先減低大影響，然後再採取適當的回應。

知識分享：要包含問題解決方法，不要只說我發生了一個中毒事件，但是我找不到問題；或者我解決問題了但沒告知我如何解決，這就不充足了。**要能夠提供相對應的解決方式，讓大家都能共享資安資源，真正做到區域聯防的概念與實質效果。**

NIST SP 800-53 Revision 4

這是資安領域裡大家常見到的一份美國國家標準，很多文件文獻都是參照這一份標準框架。它是一個基礎的準則，裡面有非常詳盡的、按照美國聯邦資訊系統訂出來的基準控制線。然後分為這些向度 (請參照圖三)，裡面實作的控制非常詳盡，甚至到你怎麼去做，要的 Sample 或細節，都可以找到參考。雖然這份文件內容是用偏向美國的角度寫的，但資訊安全不分國界，看過這些文件後會發現，其實我們都用得上，尤其有很多控制做得很好，像 NIST SP 800-53 就包含許多 ISO 27001 或一些管理框架沒講到的細節。有些單位在面臨資安法挑戰時，直接參考 ISO 27001 的附錄 A 控制項來施行，然後就覺得足夠了。但**很多單位現在在做一件事：把資訊安全管理法和 ISO 27001 做比對，去看自己實作面到底還缺什麼？缺了什麼是可以藉由其他標準再補進來。管理和架構大概我們都已經容易達成了，但實作面就可將這些更細緻的標準拉進來，作為應用。**



〈圖三〉NIST SP 800-53 標準架構與特色

落實案例：

一、「資通安全維護計畫」中的資通安全風險評估

NIST SP 800-53 CA 安全評估和授權

NIST SP 800-53 RA 風險評鑑

先談風險安全評估與授權：

制定安全評估計劃，包含：1.評估運行中的安全控制和控制增強 2.確定安全控制有效性的評估程序 3.評估環境、評估團隊和評估角色和職責。評估資訊系統及其運行環境中的安全控制、實施程度，預期運行，滿足既定安全性方面產生預期結果。記錄評估結果的安全評估報告，並向適當的人提供安全控制評估的結果。

其中，特別注意**「向適當的人提供安全評估結果」: 做了一個安全評估報告，到底要給誰看？評估不能只是拿在手上，而是要給相關做決策的人，對方才能依照你的評估報告作出正確的決策。**

再來看風險評鑑：

先做安全分類再做風險評鑑。

安全分類：根據適用的法律、行政命令、指令、政策、法規、標準和指南對資訊和資訊系統進行分類。**記錄資訊系統安全計劃中的安全分類結果。確保授權人員審查並批准安全分類決定。**

風險評鑑：(和風險的損害衝擊程度有關) 對未經授權存取、使用、揭露、破壞、修改、儲存或傳輸的資訊進行風險評鑑，**包含損害的可能性和程度**。文件化風險評鑑結果與審查風險評鑑結果。**將風險評鑑結果提供給組織內適當的人員，更新風險評鑑在資訊系統或操作環境發生重大變化 (包括識別新威脅和漏洞) 或可能影響安全狀態的其他條件。**

二、「資通安全維護計畫」中的資通安全防護及控制措施

NIST SP 800-53 AC 存取控制

NIST SP 800-53 SI 系統和資訊整合

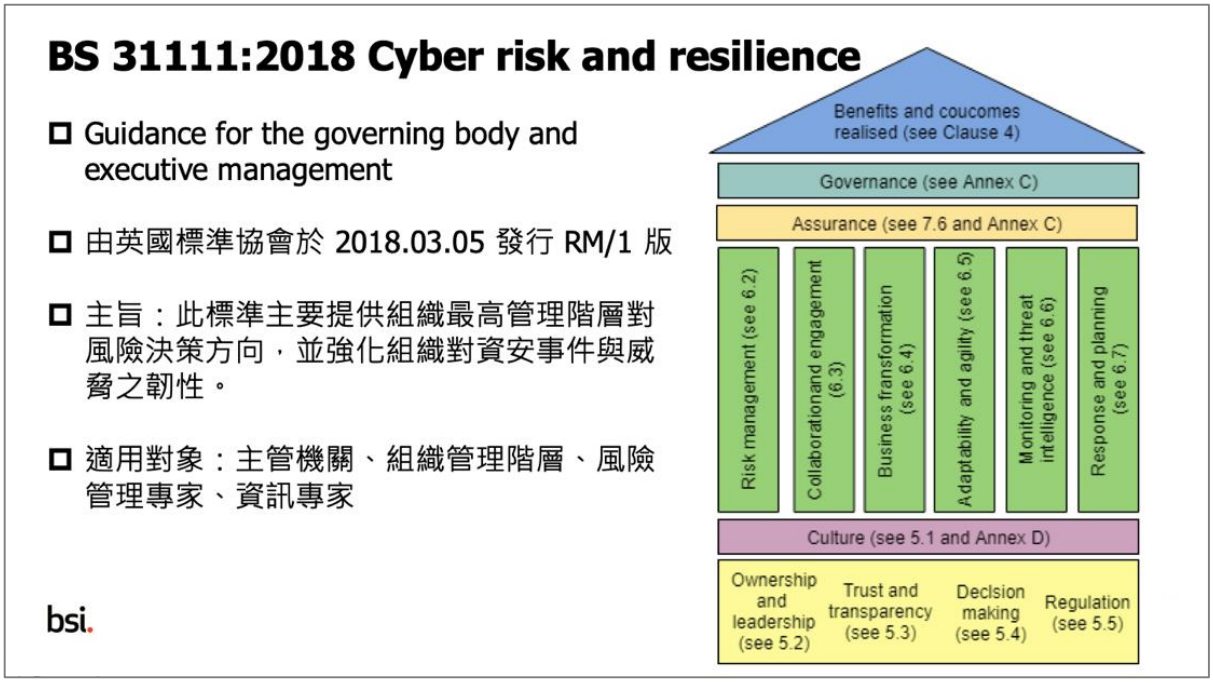
先談存取控制，對應到的是「資訊共享」: 透過使授權用戶能夠確定分配給共享人員的存取權限是否與資訊的訪問限制相同。採用自動化機制來協助資訊共享決策—**關於怎麼做限制？最好能夠用自動化機制來協助，這點是大家都沒有想到的。**

再來看系統整合。相關的是「缺陷修復」: 識別、報告和矯正資訊系統缺陷。安裝前測試與修復缺陷有關的軟硬體。在定義的時間內發佈更新，以及修復納入組織組管理流程—**關於「定義時間內發布更新」，此處特別要請業務體諒 IT：我想上 patch，但業務單位說不行，而畢竟如果漏洞風險出事了誰來負責？另外「納入組織的管理流程」，如果**

是針對資安而進行的變更，也是要請業務同仁理解 IT 為何要做這樣的變更。當然，組織變更一定要流程化才會順暢。

BS 31111:2018 Cyber risk and resilience

BS 31111 的特色是替企業從各方評鑑之後導入必要成熟度模型。在對應資訊安全管理法這部分關注在 High Level，針對主管機關，最高管理階層，要做的決策，以及風險決策的方向，強化組織對資安事件與威脅之韌性。目前提供大家參考的是 2018 年的版本，可以看到時下許多標準（包含 ISO）都走 BS 31111 這種 Annex SL 高階結構框架。



〈圖四〉BS 31111 標準架構與特色

落實案例：

一、「資通安全維護計畫」中的專責人力

> **BS 31111 7.7 Awareness and training**
>
> **應確保組織具備所需之資安知識與技能，訓練應包含明確的目標、適當的參與者、合適的資安相關內容及有效性評量。**

要請大家面對的是：您的專責人力是否有相關知識還是只是指派一個人？若他沒有專業的 Knowhow，他對整個管理制度是沒有成效的。很多單位目前就只是指派一人掛名，無法近一步深入回答，這是要請大家再重新衡量的。

二、「資通安全管理監督稽核與持續改善」

BS 31111 7.3 Evaluation

組織應持續評估資安目標是否與組織願景一致，取得資安防護有效運作之證據，確保投資與收益之平衡，可安排獨立第三方或內外部稽核人員進行審查。

BS 31111 7.4 Monitoring

組織應制定資安量測指標(KPI)並持續監控是否達到預期之目標，管理階層應定期審查並根據實務狀況調整 KPI。

要制定資安量測並對應到 KPI，角度就比較不同。要注意資安目標是否與組織願景一至，還要考慮投資與收益平衡，整體思考會稍微複雜一些。最後，可安排第三方或內外部稽核人員進行審查，以維持公正性。

結語

以上是替大家彙整出各個國際標準與資通安全管理法核心面向的對應與落實，期協助讀者對於各自的疑惑與需求獲得快速的區分與理解。所有的標準網路上均可取得相關資訊，部份會需要費用，也建議大家：**先從資通安全維護計畫著手，計劃訂出來了，要做的事情與先後順序也會清晰明朗。**像是哪些標準提供的向度控制、執行內容可以拿出來用，或是透過 BSI 訓練課程持續協助大家。

資通安全管理法於今年開始施行，為的是提升整個資通安全能量，而非讓大家綁手綁腳，並因此造就了很多的工作機會。從資安專職管理人員設置到人才培育，資通安全管理法也都有明確提出需求，產業工作機會大增、人力需求上升。資安新時代到來，BSI 也會繼續陪著老朋友新夥伴，一同迎向資安之滔滔江水勢不可擋。

BSI 資通安全管理法相關課程

ISO/IEC 27001 資訊安全管理系列課程

ISO 27001 資訊安全管理基礎課程
ISO 27001 資訊安全管理建置課程
ISO 27001 資訊安全管理內部稽核員課程
ISO 27001 資訊安全管理風險評鑑課程
ISO 27001 資訊安全管理主導稽核員課程

NIST 網路安全框架課程

NIST CSF 網路安全框架建置課程

資通安全管理法課程

資通安全管理法稽核課程

BSI 訓練學苑

T: +886 2 2656 0333 Ext. 152
E: training.taiwan@bsigroup.com

- **洽詢 BSI** ｜ 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫