淺談 NIST 網路安全框架及驗證方案

取得 ISO/IEC 27001 + NIST Cybersecurity Framework 雙驗證
持續改善資安管理並提升客戶信心

> 關鍵基礎設施受到的網路威脅持續增加，是我們必須面對的最嚴重的國家安全挑戰之一。面對這種威脅時，美國的國家和經濟安全仰賴國家基礎設施的可靠運作。
>
> —摘自美國總統歐巴馬於 2013 年 2 月簽署的第 13636 號行政命令

「關鍵基礎設施」是指對國家至關重要的系統和資產，無論是實體的還是虛擬的，這些系統和資產如果喪失能力或受到破壞，都會對安全、經濟、國家公共衛生、安全或以上各要素的組合造成破壞性的影響。

2013 年初，美國總統歐巴馬發布了第 13636 號行政命令，指示國家標準暨技術研究院（National Institute of Standards and Technology, NIST）與全球自願開發網路安全框架的相關利害關係人合作。這則行政命令還規定此框架應基於現有標準、指南和實務做法，其主旨在降低營運關鍵基礎設施之組織的網路安全風險。在過去的五年中，對關鍵基礎設施的威脅及發生之可能性一再增加，建立在其上的 NIST 框架和網路安全戰略也變得越來越重要。

NIST 框架—結構和要求

行政命令簽署後，提出全球產業網路安全需求的跨功能團隊在 NIST 的指導下，透過一系列工作研討會來建立起網路安全框架（Cybersecurity Framework, CSF）。今天，此框架提供給關鍵基礎設施和其他組織一套具有成本效益、靈活、已排定優先順序和可重複比較再生的方法來建立、應用資訊和網路安全的控制措施。

此框架是以風險為基礎，並由三個要素組成：

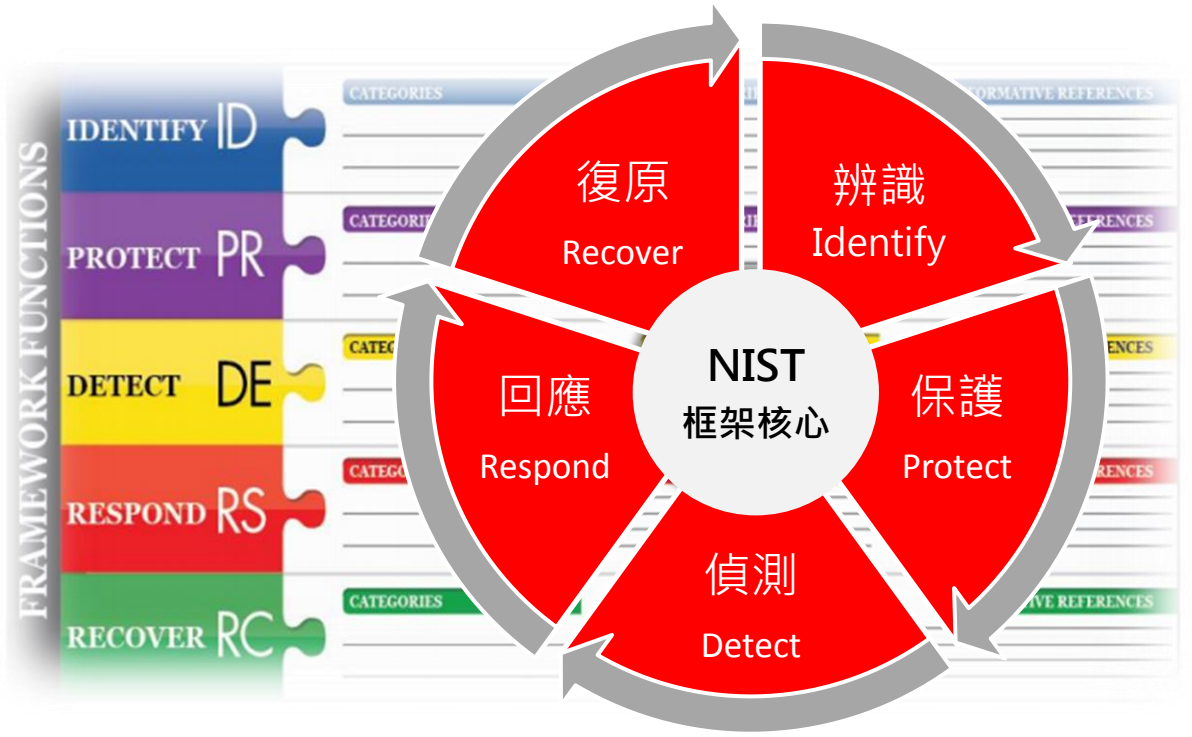
1. 框架核心（Framework Core）
2. 框架設定檔（Framework Profile）
3. 實施層級（Implementation Tiers）

框架核心包含一系列活動，可幫助組織實現特定的網路安全成果。框架核心中也從指引引用了可以用來達成這些成果的實例，並且相關關注方也肯定這些指引確實有助

於管理網路安全風險。框架核心由四個要素組成：

1. 功能（Functions）
2. 類別（Categories）
3. 次類別（Subcategories）
4. 參考資訊（Informative References）

此框架核心分為 5 種並行且持續的功能，包括：辨識（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）和復原（Recover）。



〈圖一〉 NIST 框架核心結構

綜合思考這些功能，可為網路安全生命週期和 / 或組織對其網路安全風險管理提供更高層次的策略觀點。

框架設定檔有助於將功能、類別和次類別（參見下頁〈圖二〉）對應到特定的業務要求、風險容忍度和組織資源。

框架實施層級提供有關組織如何看待網路安全風險的背景，以及所採取的風險管理流程，共分為四個層級，範圍從 Partial（層級 1）到 Adaptive（層級 4），藉由實施層級來描述日趨嚴格和複雜的網路安全風險管理實踐程度，了解依據業務需求而進行網路安全風險管理的程度，以及如何將其整合到組織整體的風險管理實務做法中。

隨著框架內所有元素的共同運作，提高了組織的資訊安全透明度，進而保護了組織的機密性以及個人隱私和公民自由。

功能	辨識 Identify	保護 Protect	偵測 Detect	回應 Respond	復原 Recover
類別	• 資產管理 • 營運環境 • 治理 • 風險評估 • 風險管理策略	• 存取控制 • 意識與教育訓練 • 資料安全 • 資訊保護與程序 • 維護 • 防護技術	• 異常與事件 • 持續性的安全監控 • 檢測流程	• 回應計畫 • 溝通 • 分析 • 緩解 • 改善	• 復原計畫 • 改善 • 溝通

〈圖二〉NIST CSF 五大功能（Functions）及其類別（Categories）

七個步驟建立與實施 NIST CSF 框架

如何判定組織的 NIST NCF 已被合理的實施？良好的網路安全計劃需要良好的風險治理。該計劃必須考慮到任何隱私衝擊，特別是考慮到 GDPR 等法規。徹底的培訓可確保組織內的個人了解自己對安全流程、程序和結果的責任並全心全力投入。人員還需要知道自己應向哪個管理層報告。

BSI 提供實施 NIST 網路安全框架的七個步驟，協助管理階層了解公司的策略方向以身作則，以實踐良好的網路安全。最高管理階層也必須支持 1) 遵守組織的網路安全流程之合規性，2) 所有適用的隱私法律和法規，和 3) 任何地方、國家和全球的法規要求。

〈圖三〉NIST 網路安全框架與治理的七步驟

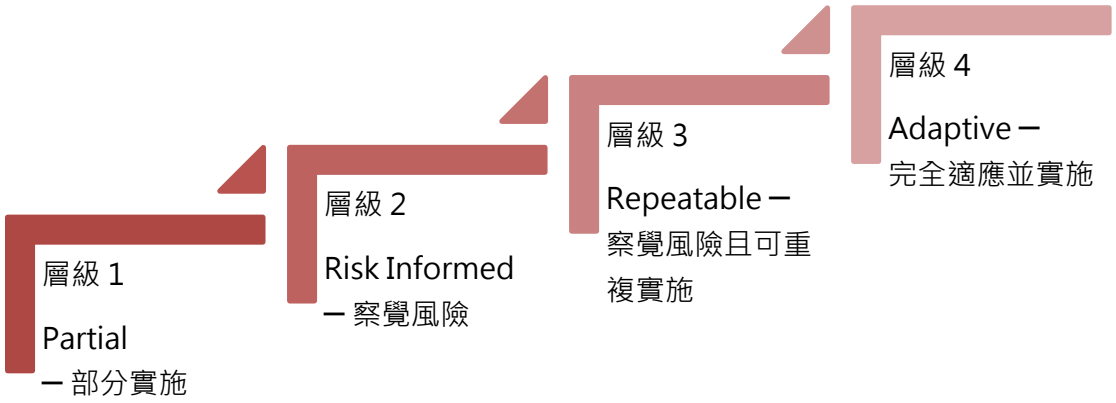
一旦實施了網路安全系統和良好治理，組織就必須進行適當的評鑑衡量，以使組織能夠持續判定新流程的有效性和適切性或改進後的網路安全所產生的價值。隨著新的網路安全威脅每天都在出現，這些評鑑衡量標準也可以提高人必要的警覺心。

證明 NIST CSF 的符合性及有效性

越來越多的組織聲稱他們符合網路安全框架；但是，沒有人對這些聲明有很大的信心。此框架旨在根據組織的需求並以高成本效益的方式來管理其網路安全風險，而不對組織施加額外的監管要求。相對的，此框架仰賴的是現有的標準、指引和實務做法，因此採用此框架的企業組織可以有更多彈性。

NIST CSF 版本 1.1 已於 2018 年 4 月發布，允許無縫整合到 ISO/IEC 27001 管理系統中以用來評估組織的安全成熟度並驗證此過程，成熟度可以藉由使用此框架結合 ISO/IEC 27001 的附錄 A 來評估差異而得出。

BSI 已提供 **NIST CSF 的驗證方案，高度結合現有的 ISO/IEC 27001 驗證，框架的驗證週期也和 ISO/IEC 27001 驗證週期同步。驗證活動除了確認 NIST NCF 的符合性之外，BSI 使用專有模型來提供與成熟度（或層級）相關的回饋意見**，共分為四個層級，從 Partial（層級 1）到 Adaptive（層級 4），以確保符合性不會成為唯一要求，彰顯組織對於網路安全的管理能力等級，以作為組織強化資訊安全治理能力和優化資源規劃的重要參考依據。



結語

依據 WEF（世界經濟論壇）於 2018 年公布的「Regional Risks for Doing Business 2018」報告，網路攻擊（cyber-attack）高居東亞及太平洋地區的區域風險第一名，不論是公部門或私人企業都應留意網路攻擊可能對組織營運帶來的重大衝擊。藉由 NIST 網路安全框架（NCF）與整合 ISO/IEC 27001 資訊安全管理系統，**任何組織皆可依據該框架評估源自於網路的資訊安全風險，及依據風險高低的排序選擇控制措施以降低風險**。對於欲積極向內外部關注方展現資訊安全治理能力的組織，藉由取得 **ISO/IEC 27001 + NIST Cybersecurity Framework 的雙重驗證**，不但可以持續改善其資訊安全的管理能力，也將顯著提升內外部關注方對其提供之資訊服務的信心。●