The NIST Cybersecurity Framework 2.0
NIST 網 路安全框架(CSF) 2.0

本出版品可從以下網址免費取得：

https://doi.org/10.6028/NIST.CSWP.29.chi

2024 年 2 月26 日

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

摘要

NIST 網路安全框架(CSF) 2.0 為產業、政府機構及其他組織提供管理網路安全風險之指引。本標準提供高標準網路安全成果之分類法，無論任何規模、行業或成熟程度之組織都適用此分類法，可以更好的理解、評鑑、優先排序及對網路安全工作進行溝通。本網路安全框架(CSF)雖無規定如何達成，但可將其連結線上資源，為達成這些成果的實務及控制提供額外的指引。本標準描述網路安全框架(CSF) 2.0 及其部分，並描述其多種使用方法中之部分方法。

關鍵字

網路安全；網路安全框架(CSF)；網路安全風險治理；網路安全風險管理；企業風險管理；剖繪；層級。

受眾(Audience)

開發及引領網路安全計畫的每個人皆為 CSF 的主要受眾。CSF 也可用於指導參與風險管理的其他人（包含執行者、董事會、專業收購人員、專業技術人員、風險管理人員、律師、人力資源專家及網路安全與風險管理稽核員）針對網路安全相關決策。此外，CSF 對於制定及影響政策的人員（例如協會、專業組織、監管者們）在建立與傳達網路安全風險管理的優先等級時，是非常有用的。

補充內容

NIST 將持續建立與代管額外的資源，以協助組織實施 CSF，包含快速入門指導與社群剖繪。所有資源均於 NIST CSF 網站上公開提供。有關可在 NIST CSF 網站上參考的其他資源建議，可隨時透過 cyberframework@nist.gov 與 NIST 進行分享。

受眾注意

除非另有註記，本標準中引述、參閱或摘錄的文件並未全部納入本標準。

在 2.0 版本前，網路安全框架被稱為「改善關鍵基礎設施網路安全框架」。但此名稱不適用於 CSF 2.0。

致謝

CSF 為美國及世界各地產業界、學術界及政府多年合作之成果。NIST 致謝且感謝

所有為修訂 CSF 提供貢獻的人。有關 CSF 開發過程之資訊可於 NIST CSF 網站上取得。也可隨時透過 cyberframework@nist.gov 與 NIST 分享使用 CSF 上的經驗。

目錄

圖示

前言

網路安全框架 (CSF) 2.0 設計用於協助各種規模與部門的組織（包含產業、政府、學術界及非營利組織）執行管理及降低網路安全風險。無論組織的網路安全計畫的成熟程度及技術複雜程度為何，CSF 皆可適用。儘管如此，CSF 仍未採納統一適用的做法。因每個組織都有共同及唯一的風險，以及不同的風險偏好及容忍度、特定任務與達成這些任務的目標。故組織在實施 CSF 的方式上必然有所不同。

在理想情況下，CSF 將用於解決網路安全風險以及企業的其他風險，包含財務、隱私、供應鏈、聲譽、技術或實體本質的風險。

CSF 的描述為使廣大受眾，包含執行者、管理者及實務者，無論他們的網路安全專業知識如何，皆可理解的預期成果。因這些成果是部門、國家及技術中立，且可為組織提供因應其唯一風險、技術及任務考量所需的靈活度。成果可直接對應潛在的安全控制措施，以立即考量緩解網路安全風險。

儘管這是非規定性的，但 CSF 是可協助使用者理解與選擇特定的成果，且不斷延伸線上資源，包含快速入門指引系列 (QSGs)，提供如何達成具體成果的建議，也有補足 CSF。此外，各種工具提供可下載的格式，以協助組織選擇將某些流程自動化。QSG 則提供初步使用 CSF 的建議方法，並邀請受眾更深入地探索 CSF 與相關資源。可藉由 NIST CSF 網站獲取 CSF 與來自 NIST 及其他機構的補充資源應視為「CSF 組合」，以協助管理與降低風險。無論如何應用，CSF 都會提示使用者在情境中考量其網路安全態勢，然後使 CSF 能夠適用其特定需求。

基於先前版本，CSF 2.0 包含強調治理與供應鏈重要性之新功能。其中特別關注 QSGs 來確保 CSF 具有相關性，且使小型組織與大型組織皆可輕易存取。NIST 目前提供實施示例及資訊參考，可於線上取得且定期更新。產生現行與目標狀態的組織剖繪，可協助組織將他們想要或需要的狀況進行比較，並可更快的實施與評鑑安全控制。

因網路安全風險不斷增加，管理這些風險必須是一個持續的過程。無論組織是剛開始面臨網路安全挑戰，或已經擁有活躍多年且經驗豐富、資源充足的網路安全團

隊，都是一樣的情況。CSF 設計對於任何類型的組織都是有價值且可長期提供適當的指引。

1. 網路安全框架(CSF)概覽

本標準為 NIST 網路安全框架（框架或 CSF）的 2.0 版。包含以下部分：

- ***CSF 核心***，CSF 的核心係高標準網路安全成果的分類，可協助任何組織管理其網路安全風險。CSF 核心部分是詳述每個成果的功能、類別及子類別之階層結構。 這些成果可被不論其網路安全專業知識為何的廣大受眾，包含執行者、管理者及實務者所理解。因成果是部門、國家及技術中立，故可為組織提供因應其唯一風險、技術及任務考量所需的靈活性。
- ***CSF 組織剖繪***，這是一種依 CSF 核心成果來描述組織目前及/或目標網路安全態勢的機制。
- ***CSF 層級***，可用於 CSF 組織剖繪，將組織之網路安全風險治理與管理實踐處理嚴謹化。層級也可為組織如何審視網路安全風險與管理這些風險的流程提供適合的地方。

本標準僅描述組織希望達成的理想成果，但無指定成果及如何達成的流程。有一套線上資源提供組織如何達成這些成果的描述，這些資源不僅補充 CSF，且可藉由 NIST CSF 網站取得。這些資源提供可用於達成成果的實務與控制的額外指引，預期在於協助組織理解、採納及使用 CSF。包含：

- *資訊參考*：指出目前的全球標準、指導綱要、框架、法規、政策等每項成果的指引來源。
- *實施示例*：說明達成每個成果的潛在方法。
- *快速入門指引*：提供有關使用 CSF 與其線上資源的可行指引，包括從先前的 CSF 版本過渡至版本 2.0。
- *社群剖繪與組織剖繪範本*：可協助組織將 CSF 實務化，且定義網路安全風險管理的優先順序

組織可使用 CSF 核心、剖繪、層級及補充資源來理解、評鑑、定優先排序及傳達網路安全風險。

- **理解與評估**：描述組織部分或全部的當前目標網路安全態勢，決定差異，並

評鑑處理這些差異的進度。

- **定優先排序**：識別、安排組織管理網路安全風險行動的優先順序，並將這些行動與組織的任務、法律及監管要求與風險管理及治理期望配合處理。
- **溝通**：提供一種通用語言，用於組織內部與外部，針對網路安全風險、能力、需求及期望進行溝通。

CSF 設計用於提供各種規模與部門組織使用，包含產業界、政府、學術界及非營利組織，而無論其網路安全計畫的成熟程度。CSF 是一種可自願採納，也可藉由政府政策與授權取得的基礎資源。CSF 的分類及參考標準、指導綱要及實務並非針對特定國家，且 CSF 的前版本已被美國國內外之許多政府及其他組織成功地使用。

CSF 應與其他資源（例如框架、標準、指導綱要、引領實務）結合使用，以更好的管理網路安全風險，並為企業層面的資訊與通訊技術（ICT）風險的整體管理提供資訊。CSF 為一靈活之框架，可適用於提供所有無論規模大小的組織使用。組織將持續面臨唯一的風險，包含不同的威脅與脆弱性、風險容忍度，及唯一的任務目標與要求。因此，組織管理風險作法及其 CSF 的實施將有所不同。

本標準其餘部分之結構如下：

- 第 2 節解釋 CSF 核心之基礎：功能、類別、子類別。
- 第 3 節定義 CSF 剖繪與層級之概念。
- 第 4 節提供 CSF 線上資源套件的選取部分概觀：資訊參考、實施示例及快速入門指引。
- 第 5 節討論組織如何整合 CSF 與其他風險管理計畫。
- 附錄 A 為 CSF 核心。
- 附錄 B 包含 CSF 層級的概念性說明。
- 附錄 C 為 CSF 術語之專用詞彙。

2. CSF 核心簡介

附錄 A 為 CSF 核心—如圖 1 所示，一組依功能、類別、子類別排序的網路安全成果。這些成果並非執行的檢查表；為達成成果而採取的特定措施將依組織與使用案

例的不同而有所不同，而個別負責這些措施的人員也將有所不同。此外，核心中功能、類別及子類別的順序與大小，並不代表著達成的順序或重要性。核心的架構希望能夠引起組織內負責實施風險管理人員的最大共鳴度。

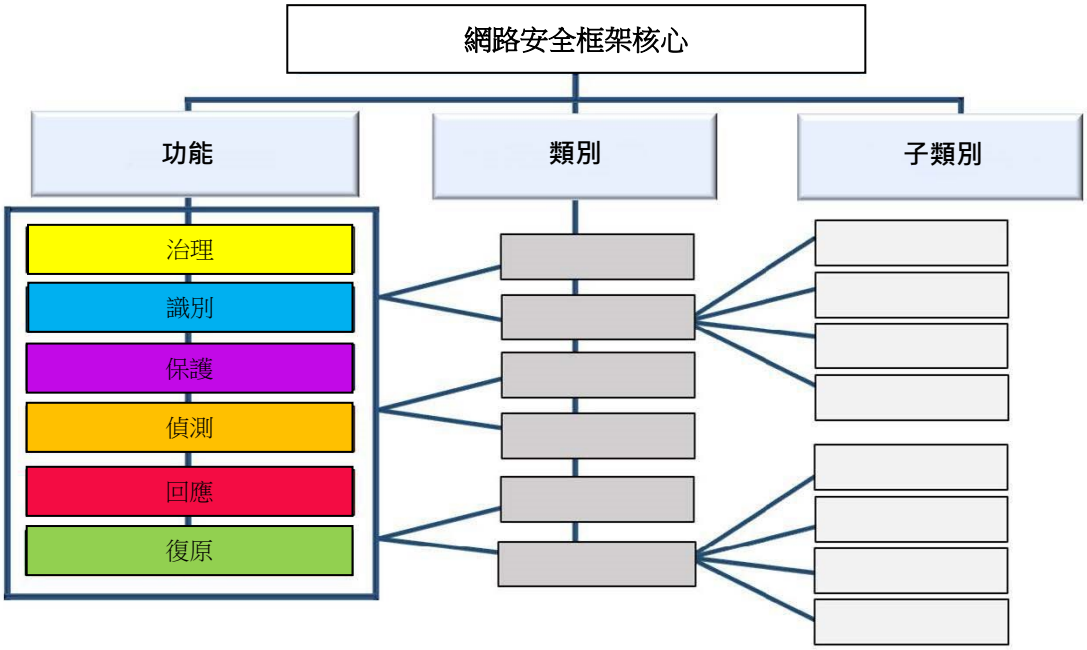

圖 1. CSF 核心架構

CSF 核心功能—治理、識別、保護、偵測、回應及復原—於最高層級組織網路安全之成果。

- **治理(GV)** — *建立、傳達及監視組織之網路安全風險管理策略、期望及政策。* 治理功能提供成果，用於告知組織如何在其任務與利害關係者期望下達成，且針對其他五個功能之成果定優先排序。對於將網路安全納入更廣泛企業風險管理(ERM)策略之組織而言，治理活動是為關鍵。治理致力於加強組織環境的理解；建立網路安全策略與網路安全供應鏈風險管理；角色、責任及權限；政策及網路安全策略之監督。
- **識別(ID)**–*用於理解組織當前之網路安全風險。*理解組織資產(例如資料、硬體、軟體、系統、設備、服務、人員)供應者及相關網路安全風險，使組織依其風險管理策略與治理，以識別任務需求來確定優先排序。此功能亦包含識別組織支援網路安全風險管理之政策、計畫、流程、程序與實務的改善機會，為所有六個功能提供資訊。

- **保護(PR)**–*使用保護措施來管理網路安全風險*。當資產與風險被識別及定出優先排序時，保護(PROTECT)支援保全這些資產之能力，以防止或降低不利網路安全事件發生的可能性與衝擊，並增加利用機會的可能性及影響。此功能涵蓋的成果包含身分管理、鑑別及存取控制；認知與訓練；資料安全；平台安全（例如實體與虛擬平台上之硬體、軟體及服務）；與技術基礎設施的強韌性。
- **偵測(DE)**–*尋找並分析可能的網路安全攻擊與危害*。偵測可即時發現及分析異常情況、危害指標，且可能找出正在發生的網路安全攻擊與事件之其他潛在不利網路安全事件。此功能支援成功的事故回應與復原活動。
- **回應(RS)**–*針對偵測到的網路安全事件採取行動*。回應支援能力包含網路安全事件的效應。此功能之成果涵蓋事件管理、分析、緩解、報告及溝通。
- **復原(RC)**-*恢復因網路安全事件衝擊之資產與運行*。復原(RECOVER)需支援即時恢復正常運行，以減少網路安全事故之效應，並於復原工作期間維持適當的溝通。

儘管許多網路安全風險管理活動著重於預防負面事件的發生，但其實也可支援利用正面機會。降低網路安全風險的行動可能會以其他方式使組織受益，像增加收入（例如，首先向商業代管提供者提供多餘的設施空間，用於代管他們自己與其他組織的資料中心，然後將主要財務系統從組織的內部轉移至資料中心，並交由代管提供者代管以減少網路安全風險）。

圖 2 將 CSF 功能顯示為一個圓輪，因其所有功能都彼此相關。例如，組織將於識別(IDENTIFY)下對資產進行分類，並在保護(PROTECT)下採取步驟以保全資產。針對治理(GOVERN)與識別(IDENTIFY)功能之計畫及測試投資報酬率，將支援在偵測(DETECT)功能中的即時偵測，與回應(RESPOND)及復原(RECOVER)功能中之網路安全事故的即時回應與復原行動。治理(GOVERN)位於圓輪中心，係因其需告知組織將如何實施其他五項功能。

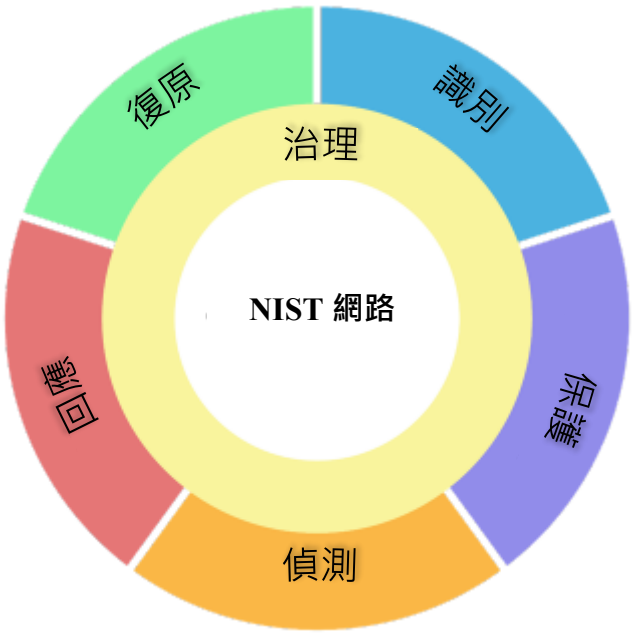

圖 2. CSF 功能

這些功能應同時因應。支援治理(GOVERN)、識別(IDENTIFY)、保護(PROTECT)及偵測(DETECT)的行動都應持續發生，且支援回應(RESPOND)與復原(RECOVER)之行動也應隨時待命，並於網路安全事故發生時啟動作用。所有功能都在網路安全事故面發揮重要作用。治理(GOVERN)、識別(IDENTIFY)及保護(PROTECT)的成果將可協助於預防與預備事故，而治理(GOVERN)、偵測(DETECT)、回應(RESPOND)及復原(RECOVER)成果則可協助發現與管理事故。

每個功能皆以匯總其內容的動詞來命名。每個功能可區分為多個*類別*，這些類別是共同構成此功能之相關網路安全成果。*子類別*可進一步將每個類別畫分為更具體的技術與管理活動成果。子類別雖無法窮舉，但可描述支援每個類別的詳細成果。

功能、類別及子類別適用於組織使用的所有 ICT，包含資訊科技 (IT)、物聯網 (IoT)及運作技術(OT)。它們也適用於所有類型的技術環境，包含雲端、行動及人工智慧系統。CSF 核心具有前瞻性，且預期可適用於未來技術與環境的變化。

3. CSF 剖繪與層級簡介

本節定義 CSF 剖繪與層級之概念。

3.1 CSF 剖繪

*CSF 組織剖繪*係依核心成果來描述組織現行及/或標的網路安全態勢。組織剖繪藉由考量組織的任務目標、利害關係者的期望、威脅全景及要求來理解、裁適、評鑑、定優先排序及傳達核心成果。因此組織便可將其行動定優先順序以達成特定成果，且同步將資訊傳達給利害關係者。

每個組織剖繪都應包含以下之一項或兩項要素：

1. *現行剖繪*指定組織目前正在達成（或試圖達成）的核心成果，且描述如何達成每個成果的方式或程度。
2. *標的剖繪*指定組織為達成其網路安全風險管理目標，而選擇與定優先排序的期望成果。標的剖繪考量組織網路安全態勢的預期變化，如新要求、新技術採納及威脅情報趨勢。

> *社群剖繪*是用於建立與發布 CSF 成果的基準，以因應多個組織之間共同的利益和目標。社群剖繪通常是針對特定部門、子部門、技術、威脅類型或其他使用案例而開發。組織可以使用社群剖繪作為自己標的剖繪的基礎。社群剖繪的示例可於 NIST CSF 網站上尋找。

圖 3 所示及下面總結的步驟，說明組織可使用組織剖繪來協助持續改善其網路安全的一種方法。

圖 3. 建立及使用 CSF 組織剖繪之步驟

1. **組織剖繪之適用範圍。**剖繪應基於其高階事實與假設的文件來定義其適用範圍。一個組織可依需求擁有任意多個不同適用範圍之組織剖繪。例如，剖繪可因應整個組織，也可涵蓋組織的財務系統，或對抗勒索軟體威脅並處理涉及這些財務系統的勒索軟體事故。
2. **蒐集準備組織剖繪所需資訊。**資訊示例可能包含組織政策、風險管理優先排序及資源、企業風險剖繪、營運衝擊分析 (BIA) 登錄、組織遵循的網路安全要求事項及標準、實務與工具（例如程序與保障措施）以及工作角色。
3. **建立組織剖繪。**決定剖繪應包含所選 CSF 成果中哪些類型的資訊，並記錄所需的資訊。考量目前剖繪蘊含的風險，以告知標的剖繪之規畫與優先排序。此外，請考量使用社群剖繪作為標的剖繪的基準。
4. **分析現行與標的剖繪間的差異，並建立行動計畫。**執行差異分析，以識別及分析現行與標的剖繪之間的差異，並開發優先行動計畫（例如風險登錄、風險詳細報告、行動計畫及時程 [POA&M]），以因應這些差異。
5. **實施行動計畫，並更新組織剖繪。**遵循行動計畫以因應差異，並使組織朝著標的剖繪前進。行動計畫可能有一個整體期限或已在進行中。

基於持續改善的重要性，組織可依需求時常重複進行這些步驟。

組織剖繪還有其他的用途。例如，現行剖繪可用於記錄並與外部的利害關係者，傳

達組織的網路安全能力與已知之改善機會，例如業務夥伴或潛在客戶。此外，標的剖繪可協助向供應者、夥伴及其他第三方表達組織網路安全風險管理的要求及期望，作為達成的目標。

3.2 CSF 層級

組織可以選擇使用層級來告知現行及標的剖繪。層級係將組織的網路安全風險治理與管理實務的嚴格性進行特性化，並為組織如何審視網路安全風險與管理這些風險的過程提供各種情境。如圖 4 所示及附錄 B 中的概念性說明，這些層級反映組織管理網路安全風險的實務，如部分（層級 1）、風險告知（層級 2）、可重複（層級 3）及適應性（層級 4）。這些層級描述過程從非正式的、臨時的回應至敏捷的方法、告知風險及持續改善。層級的選擇可協助組織如何管理其網路安全風險設定整體基調。

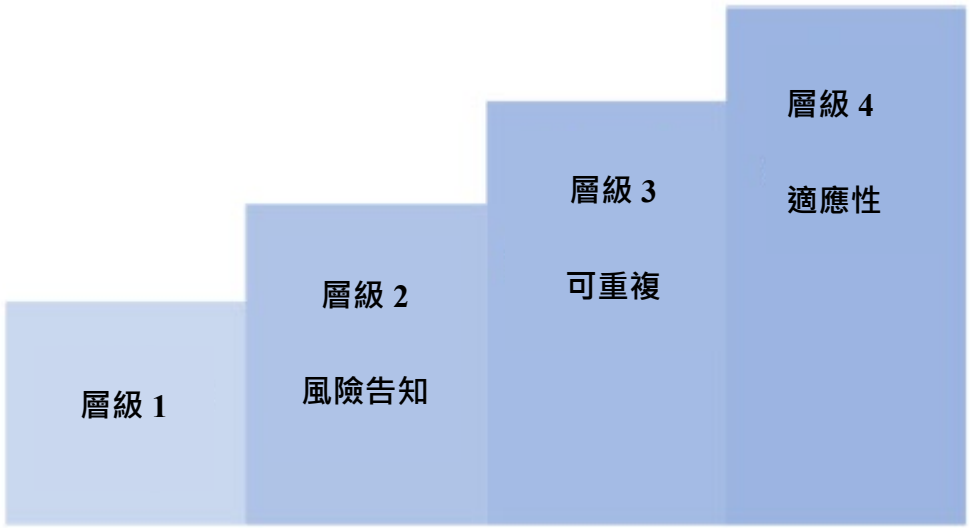

圖 4. 網路安全風險治理與管理之 CSF 層級

層級應用於補充組織的網路安全風險管理方法論，而非取代。例如，組織可使用層級進行內部溝通，當作管理網路安全風險的組織範圍內之方法評估效果。當風險或命令較大時，或當成本效益分析顯示可降低負面網路安全風險且具有成本效益時，可鼓勵升至更高的層級。

NIST CSF 網站提供有關使用剖繪與層級的更多資訊。包含 NIST 代管的組織剖繪範本的指標，以及各種機器可讀與人類可用格式的社群剖繪儲存庫。

4. CSF 的線上補充資源簡介

NIST 與其他組織產生一套線上資源，用於協助組織理解、採納及使用 CSF。因採線上代管的方式，因此這些額外資源可比本標準更頻繁地進行更新，本標準不會經常更新的原因是為了向使用者提供穩定度，並以機器可讀的格式提供。本節提供概述三種類型之線上資源概覽：資訊參考、實施示範及快速入門指導。

資訊參考用於指示核心與各種標準、指引綱要、法規及其他內容之間關係對應。 資訊參考可協助於告知組織如何達成核心成果。資訊參考也可用於部門或特定於技術。它們可能由 NIST 或其他組織所產生。部分資訊參考的範圍甚至比子類別更窄。例如，SP 800-53，資訊系統及組織之安全與隱私控制，其中的特定控制措施可能是達成一個子類別中所述成果所需的眾多參考之一。其他資訊參考可能是更高等級，如部分因應許多子類別政策的要求事項。當使用 CSF 時，組織可識別最相關的資訊參考。

實施示例提供簡潔、行動導向步驟的概念性示例，以協助達成子類別的成果。用於表達示例的動詞包含共享、記錄、開發、執行、監視、分析、評鑑及練習。這些示例並不是組織為達成成果而可採取所有行動的綜合列表，也不代表因應網路安全風險所需行動的基準線。

快速入門指引(QSG) 是針對特定 CSF 相關主題的簡短文件，通常也對特定受眾進行調整。QSG 可協助組織實施 CSF，因其會將 CSF 的特定部分精煉為可操作的「第一步」，組織可在改善網路安全態勢與相關風險管理的過程中考量這些步驟。 這些指引會在自己的時間框架內進行修訂，並依需要新增新的指引。

有關 CSF 2.0 的新資訊參考建議可隨時透過 olir@nist.gov 與 NIST 分享。建議若需在 NIST CSF 網站上參考其他資源，包含其他的 QSG 主題，請寄信至 cyberframework@nist.gov。

5. 改善網路安全風險之溝通與整合

CSF 的使用是依組織的唯一任務與風險而有所不同。藉由理解利害關係者的期望與風險偏好及容忍度（如於 GOVERN 的概述），組織可優先考量網路安全活動，以便在網路安全支出與行動中做出明智的決定。組織可選擇以一種或多種方式處理風險，包含緩解、轉移、避免或接受負面風險，以及實現、分享、增強或接受正面風險，皆取決於潛在的衝擊與可能性。重點在於，組織可於內部使用 CSF 來管理其網路安全能力，也可於外部使用 CSF 來監督第三方或與第三方進行溝通。

無論 CSF 的使用為何，組織使用 CSF 作為指引有益於協助理解、評鑑、定優先排序、傳達網路安全風險與管理這些風險的行動。選定的成果也可用於關注與實施策略決策，以改善網路安全態勢並保持任務基本功能的連續性，同時也考量優先順序與可用的資源。

5.1. 網路安全風險之溝通改善

CSF 為改善網路安全期望、計畫及資源的溝通提供基準。CSF 促進關注組織優先排序與政策方向的執行者且可能影響達成這些優先排序的特定網路安全風險的管理者之間的雙向資訊流向（如圖 5 上半部所示）。CSF 也支援管理者與實施及運作技術的實務者之間類似的資訊流向（如圖 5 下半部所示）。此圖的左側顯示實務者與管理者及執行者分享其更新、見解及關注事項的重要性。

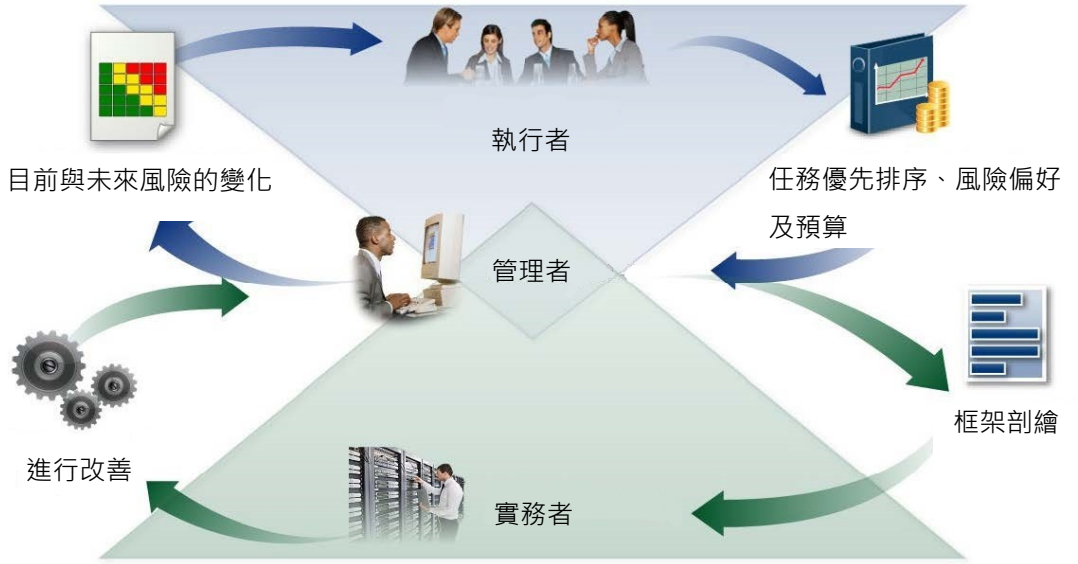

圖 5. 使用 CSF 改善風險管理之溝通

準備建立和使用組織剖繪涉及從執行者蒐集有關組織優先等級、資源及風險方向資訊。然後，管理者與開業者(practitioners)合作以溝通營運需求，且建立風險已知的組織剖繪。管理者與開業者將採取行動以縮小現行剖繪及標的剖繪之間的差異，且為系統級別計畫提供關鍵輸入。隨著整個組織達成目標狀態，包含藉由在系統層級應用的控制與監視，可藉由風險名冊及進度報告來共享更新的結果。作為持續評鑑的一部分，管理者從中獲得觀點來做出調整，可進一步減少潛在危害並增加潛在利益。

治理(GOVERN)功能用於支援與**執行者**進行組織風險溝通。執行者的討論涉及策略，特別是可能影響組織目標達成的網路安全相關不確定性。這些治理討論支援有關風險管理策略的對談與協議（包含網路安全供應鏈風險）；角色、責任及權限；政策與監督。當執行者依這些需求建立網路安全優先事項與目標時，便會傳達預期風險偏好、責任及資源。執行者也須負責將網路安全風險管理與 ERM 計畫與較低層級的風險管理計畫整合（請參閱第 5.2 節）。圖 5 上半部所反應的溝通可包含考量 ERM 與較低層級的計畫，因而可對管理者與開業者提供資訊。

執行者設定的整體網路安全目標需串接傳遞至**管理者**。在商業個體中，這些可能適用於商業線或營運部門。對於政府個體來說，這些可能是部門或分支機構層級需考

量。在實施 CSF 時，管理者將重點關注如何藉由共同服務、控制及協作來達成風險目標，如標的剖繪中所表達與透過追蹤行動計畫中的活動來改善（例如風險登錄、風險詳細報告、POA&M）。

開業者專注於實施目標狀態並測量營運風險的變化，以協助規畫、執行及監視特定網路安全活動。當實施控制措施以將風險管理在可接受的水平時，開業者向管理者與執行者提供所需資訊（例如關鍵績效指標、關鍵風險指標），以瞭解組織的網路安全態勢、做出明智的決定以及維護或調整風險相對應策略。執行者還可將此網路安全風險資料與整個組織中其他類型風險資訊結合。隨著週期的重複，期望與優先排序的更新將包含於組織剖繪更新中。

5.2. 與其他風險管理計畫之整合改善

每個組織都面臨多種類型的 ICT 風險（例如隱私、供應鏈、人工智慧），並且可能使用特定各種風險的框架及管理工具。某些組織使用 ERM 將 ICT 及所有其他的風險管理工作在高層級上進行整合，而其他組織則會將這些工作分開，來確保對每項工作具備足夠的關注。小型組織本質上可能會在企業層級進行風險監視，而大型的公司可能會將單獨的風險管理工作整合至 ERM 中。

組織可採用 ERM 方法來平衡風險考量之組合，包含網路安全，並做出明智的決策。執行者在將治理與風險策略之先前使用 CSF 結果進行整合時，會收到有關現行與計劃的風險活動之重要意見。CSF 可協助組織將網路安全與網路安全風險管理術語轉換為執行者管能夠理解的通用風險管理語言。

描述網路安全風險管理與 ERM 之間相互關係的 NIST 資源包含：

- *NIST 網路安全框架 2.0 – 企業風險管理快速入門指引*
- NIST 部門間之報告 (IR) 8286，*整合網路安全與企業風險管理 (ERM)*
- IR 8286A，*識別與估計企業風險管理的網路安全風險*
- IR 8286B，*定企業風險管理的網路安全風險之優先排序*
- IR 8286C，*為企業風險管理與治理監督進行分階段的網路安全風險管理*
- IR 8286D，*使用業務衝擊分析告知風險優先排序與回應*

- SP 800-221，*資訊與通訊科技風險對企業的衝擊：治理與管理企業風險組合中的 ICT 風險計畫*
- SP 800-221A，*資訊與通訊技術 (ICT) 風險成果：將 ICT 風險管理計畫與企業風險組合進行整合*

組織也可能發現 CSF 有利於將網路安全風險管理與個別 ICT 風險管理計畫整合，例如：

- **網路安全風險管理與評鑑**：CSF 可與已建立的網路安全風險管理及評鑑計畫進行整合，例如 SP 800-37，*資訊系統與組織的風險管理框架*，以及 SP 800-30，從 NIST 風險管理框架(RMF)的*引導風險評鑑指引*。對於使用 NIST RMF 與其發行套組出版品來說，CSF 可用於從 SP 800-53 中，*資訊系統與組織之安全與隱私控制*，補充 RMF，選擇並將控制措施定優先排序的方法。
- **隱私風險**：儘管網路安全與隱私是個別的規則，但它們的目標在某些情況下是重疊，如圖 6 所示。

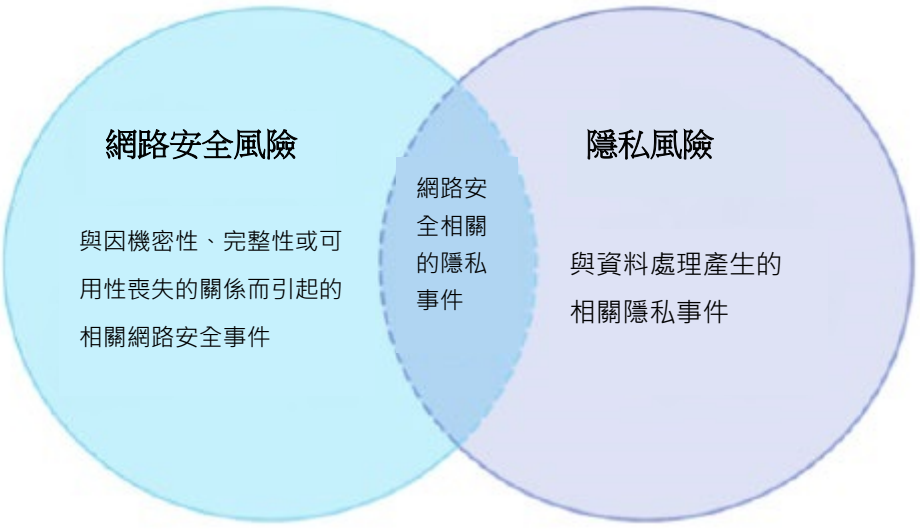

圖 6. 網路安全及隱私風險之關係

網路安全風險管理對於因應與個人資料機密性、完整性及可用性喪失相關的隱私風險是不可或缺的。例如，資料外洩可能導致身分盜竊。然而，與網路安全事故無關的方式也可能產生隱私風險。

組織處理資料係為達成任務或業務目的，但有時可能會引發隱私事件，個人

可能會因資料處理而遇到問題。這些問題可用許多方式表示，但 NIST 將其描述為從尊嚴型影響（例如尷尬或恥辱）到更明顯的傷害（例如歧視、經濟損失或身體傷害）。NIST 隱私框架與網路安全框架可一起使用來因應網路安全及隱私風險的不同面向。此外，NIST 的隱私風險評鑑方法論 (PRAM) 還提供用於隱私風險評鑑的示例問題目錄。

- **供應鏈風險**：組織可使用 CSF 來促進網路安全風險監督及與整個供應鏈中利害關係者的溝通。所有類型的技術都依賴一個複雜、全球分佈、廣泛、相互關聯的供應鏈生態系統，其路線分佈在不同的地區，且具有多層級的委外處理。該生態系統由公共的與私人的部門個體（例如獲取者、供應者、開發者、系統整合者、外部系統服務提供者及其他技術相關服務提供者）組成，這些相互作用的個體以研究、開發、設計、製造、獲取、交付、整合、操作、維護、毀棄及以其他方式利用或管理技術產品和服務。這些互動受到技術、法律、政策、程序及實踐的塑造和影響。

  基於該生態系統中複雜且相互關聯的關係，供應鏈風險管理 (SCRM) 對於組織是關鍵的。網路安全 SCRM (C-SCRM) 是一個用於管理整個供應鏈中暴露的網路安全風險，並開發適當之回應策略、政策、過程及程序的系統化過程。CSF C-SCRM 類別 [GV.SC]中的子類別提供單純關注網路安全與關注 C-SCRM 的成果間的連接。SP 800-161r1（修訂版 1），*系統與組織的網路安全供應鏈風險管理實務*，提供有關 C-SCRM 的深入資訊。

- **新興技術帶來的風險**：隨著新技術和新技術應用的出現，新的風險變得常見。當前的一個示例為人工智慧（AI），它存在網路安全與隱私風險及許多其他類型的風險。NIST 人工智慧風險管理框架 (AI RMF) 的開發便是為了協助因應這些風險。沿著其他企業風險（例如金融、網路安全、聲譽及隱私）處理人工智慧風險將產生更整體的成果與組織效率。網路安全與隱私風險管理的考量及作法適用於 AI 系統的設計、開發、部署、評估及使用。AI RMF 核心使用功能、類別及子類別來描述 AI 成果並協助與 AI 相關的管理風險

附錄 A CSF 核心

本附錄描述 CSF 核心的功能、類別及子類別。表 1 列出 CSF 2.0 核心功能與類別名稱及唯一字母識別碼。列表中的每個功能名稱都連結到附錄的部分。核心的功能、類別及子類別的順序不是依字母順序排列的；其意圖在引起組織內負責實施風險管理人員的最大共鳴度。子類別的編號刻意不依序；編號中的空白表示 CSF 1.1 子類別已在 CSF 2.0 中重新定位。

表 1. CSF 2.0 核心功能及類別名稱與識別符

功能	類別	類別識別碼
治理(GV)	組織情境	GV.OC
	風險管理策略	GV.RM
	角色、職責及權限	GV.RR
	政策	GV.PO
	監督	GV.OV
	網路安全供應鏈風險管理	GV.SC
識別(ID)	資產管理	ID.AM
	風險評鑑	ID.RA
	改善	ID.IM
保護(PR)	身分管理、鑑別及存取控制	PR.AA
	認知及訓練	PR.AT
	資料安全	PR.DS
	平台安全	PR.PS
	技術基礎設施抗障程度	PR.IR
偵測(DE)	持續監視	DE.CM
	不良事件分析	DE.AE
回應(RS)	事故管理	RS.MA
	事故分析	RS.AN
	事故回應報告及溝通	RS.CO
	事故緩解	RS.MI
恢復(RC)	事故復原計畫執行	RC.RP
	事故復原溝通	RC.CO

CSF 核心、資訊參考及實施示例可在 CSF 2.0 網站上與藉由 CSF 2.0 參考工具取得，此工具容許使用者探索，並以人類與機器可讀的格式匯出。CSF 2.0 核心也提供類似 CSF 1.1 的傳統格式。

治理 (GV)：建立、傳達及監視組織的網路安全風險管理策略、期望及政策。

- **組織情境 (GV.OC)**：瞭解圍繞組織網路安全風險管理決策的情境—任務、利害關係者期望及法律、監管及合約要求事項。
  - **GV.OC-01**：理解組織任務並告知其網路安全風險管理。
  - **GV.OC-02**：理解內部與外部之利害關係者，並考量其對網路安全風險管理的需求與期望。
  - **GV.OC-03**：理解並管理有關網路安全的法律、監管及契約要求事項—包含隱私與公民自由義務。
  - **GV.OC-04**：理解並傳達外部利害關係者依賴或期望從組織獲得的關鍵目標、能力及服務。
  - **GV.OC-05**：理解並傳達組織所依賴的成果、能力及服務。
- **風險管理策略(GV.RM)**：建立、傳達並使用組織的優先事項、限制、風險容忍度及偏好敘述和假定，來支援風險決策的操作。
  - **GV.RM-01**：由組織利害關係者建立並同意風險管理目標。
  - **GV.RM-02**：建立、傳達並維護風險偏好及風險容忍度敘述。
  - **GV.RM-03**：網路安全風險管理活動與成果包含在企業風險管理過程中。
  - **GV.RM-04**：建立並傳達描述適當風險應對選項的策略方向。
  - **GV.RM-05**：在組織內建立溝通線以應對包含來自供應者及其他第三方的網路安全風險。
  - **GV.RM-06**：建立並傳達網路安全風險的計算、記錄、分類及定優先排序的標準化做法。
  - **GV.RM-07**：將策略機會(即正向風險)特性化，並納入組織網路安全風險討論中。
- **角色、職責及權限 (GV.RR)**：建立並傳達網路安全角色、職責和權限，以促進可歸責性、績效評鑑與持續改善。
  - **GV.RR-01**：針對網路安全風險及培養具風險意識、道德及持續改進之文化，組織領導階層應負責且當責。
  - **GV.RR-02**：建立、溝通、理解及執行與網路安全風險管理相關的角色、責任及權限。
  - **GV.RR-03**：依網路安全風險策略、角色、職責及政策，分配足夠的資源。

- **GV.RR-04**：網路安全納入人力資源實務。

- **政策 (GV.PO)**：建立、傳達及執行組織之網路安全政策。
  - **GV.PO-01**：依組織情境、網路安全策略及優先順序來建立網路安全風險管理的政策、過程及程序，進行溝通與執行。
  - **GV.PO-02**：審查、更新、溝通與執行用於管理網路安全風險的政策、過程及程序，以回應需求、威脅、技術和組織使命的變化。

- **監督 (GV.OV)**:組織範圍內的網路安全風險管理活動及績效結果，用於告知、改善及調整風險管理策略。
  - **GV.OV-01**：審視網路安全風險管理策略成果，以告知及調整策略和方向。
  - **GV.OV-02**：審視及調整網路安全風險管理策略，以確保涵蓋組織要求事項及風險。
  - **GV.OV-03**：評估與審視組織網路安全風險管理績效以進行必要的調整。

- **網路安全供應鏈風險管理（GV.SC）**：網路供應鏈風險管理過程由組織利害關係者識別、建立、管理、監視及改善。
  - **GV.SC-01**：組織利害關係者建立且同意網路安全供應鏈風險管理計畫、策略、目標、政策及過程。
  - **GV.SC-02**：在內部與外部建立、溝通與協調供應者、客戶及合作夥伴之網路安全角色與職責。
  - **GV.SC-03**：網路安全供應鏈風險管理整合網路安全及企業風險管理、風險評鑑及改善過程。
  - **GV.SC-04**：供應者已知並依關鍵性決定優先排序。
  - **GV.SC-05**：建立解決供應鏈中網路安全風險的要求，確定優先級，並將其納入與供應商和其他相關第三方的合約和其他類型的協議中。
  - **GV.SC-06**:在建立正式的供應者或其他第三方關係前執行規畫及盡責查證以降低風險。
  - **GV.SC-07**：在關係過程中被識別、記錄、定優先排序、評鑑、回應及監視供應者、其產品與服務及其他第三方帶來的風險。
  - **GV.SC-08**:相關供應者及其他第三方參與事故計畫、回應及恢復活動。
  - **GV.SC-09**：供應鏈安全實務已整合至網路安全及企業風險管理計畫，並於整個技術產品及服務生命週期中監視其績效。
  - **GV.SC-10**:網路安全供應鏈風險管理計畫包含對簽訂合作夥伴關係或服務協定後發生活動的條款。

識別 (ID)：理解組織目前的網路安全風險

- **資產管理 (ID.AM)**：使組織可達成業務目標的資產 (例如資料、硬體、軟體、系統、設施、服務、人員) 並依其對組織目標及組織風險策略的相對重要性進行識別與管理。
    - **ID.AM-01**：維護組織管理的硬體清冊。
    - **ID.AM-02**：維護組織管理的軟體、服務及系統的清冊。
    - **ID.AM-03**：維護組織授權的網路通訊及內部與外部網路資料流的表示。
    - **ID.AM-04**：維護供應者提供的服務清冊。
    - **ID.AM-05**：依分類、重要性、資源及對任務衝擊定資產的優先排序。
    - **ID.AM-07**：維護指定資料類型的資料清冊及相應的詮釋資料。
    - **ID.AM-08**：系統、硬體、軟體及服務在其整個生命週期內進行管理。
- **風險評鑑 (ID.RA)**：組織用於理解組織、資產及個人面臨之網路安全風險。
    - **ID.RA-01**：識別、驗證及記錄資產中的脆弱性。
    - **ID.RA-02**：從資訊共享論壇及來源接收網路威脅情報。
    - **ID.RA-03**：識別並記錄組織的內部及外部威脅。
    - **ID.RA-04**：識別並記錄利用脆弱性威脅的潛在衝擊及可能性。
    - **ID.RA-05**：威脅、脆弱性、可能性及衝擊，以用於決定風險並告知風險優先排序。
    - **ID.RA-06**：選擇、定優先排序、規畫、追蹤及傳達風險回應。
    - **ID.RA-07**：管理變更及例外情況、評鑑風險衝擊、記錄及追蹤。
    - **ID.RA-08**：建立接收、分析及回應脆弱性揭露的過程。
    - **ID.RA-09**：在獲取和使用前評鑑硬體和軟體的真確性及完整性。
    - **ID.RA-10**：在獲取前對關鍵供應者進行評鑑。
- **改善 (ID.IM)**：在所有 CSF 功能中識別組織網路安全風險管理過程、程序及活動的改善。
    - **ID.IM-01**：從評估中識別改善。
    - **ID.IM-02**：藉由包含與供應者及相關第三方協調進行的安全測試及練習，來識別改善地方。
    - **ID.IM-03**：從營運過程、程序及活動的執行中識別改善地方。
    - **ID.IM-04**：建立、傳達、維護及改善影響營運的事故應變計畫及其他網路安全計畫。

保護（PR）：使用管理組織的網路安全風險之保障措施。

- **身分管理、鑑別及存取控制 (PR.AA)**：對實體及邏輯資產的存取僅限於授權使用者、服務及硬體，並依未經授權存取的評鑑風險進行相應的管理。
  - **PR.AA-01**：由組織來管理授權使用者、服務及硬體的身分及憑證。
  - **PR.AA -02**：依互動的情境對身分進行證明並綁定至憑證。
  - **PR.AA-03**：鑑別使用者、服務及硬體。
  - **PR.AA-04**：身分判定受到保護、傳遞及驗證。
  - **PR.AA-05**：存取權限、權利及授權在策略、管理、執行及審查中定義，並納入最小特權及職責分離原則
  - **PR.AA-06**：依風險對資產的實體存取進行相應的管理、監視與強制執行
- **•認知及訓練（PR.AT）**：為組織的人員提供網路安全認知及訓練，以利執行與網路安全相關的任務。
  - **PR.AT-01**：提供使用者認知及訓練，使其具備執行通用任務並考量安全風險的知識及技能。
  - **PR.AT-02**：為擔任特殊化的個人提供認知及訓練，使其具備在考慮安全風險的情況下執行相關任務的知識及技能。
- **資料安全 (PR.DS)**：依組織的風險策略對資料進行管理，以保護資訊的機密性、完整性及可用性。
  - **PR.DS-01**：靜態資料的機密性、完整性及可用性受到保護。
  - **PR.DS-02**：保護傳輸中資料的機密性、完整性和可用性。
  - **PR.DS-10**：保護使用中資料的機密性、完整性及可用性。
  - **PR.DS-11**：建立、保護、維護及測試資料備份。
- **平台安全（PR.PS）**：實體服務及虛擬平台的硬體、軟體（例如韌體、作業系統、應用程式）和管理與組織的風險策略一致，以保護其機密性、完整性及可用性。
  - **PR.PS-01**：建立並應用組態管理實踐。
  - **PR.PS-02**：依風險對軟體進行相關的維護、更換及刪除。
  - **PR.PS-03**：依風險對硬體進行相關的維護、更換及刪除。
  - **PR.PS-04**：產生日誌記錄並可用於持續監視。
  - **PR.PS-05**：防止提供安裝及執行未經授權的軟體。
  - **PR.PS-06**：保全整合軟體開發實務及在整個軟體開發生命週期中監視其效能。

- **技術基礎設施抗故障性 (PR.IR)**：藉由組織風險策略進行安全架構管理，以保護資產的機密性、完整性、可用性及組織的抗故障性。
  - **PR.IR-01**：保護網路與環境免受未經授權的邏輯存取和使用。
  - **PR.IR-02**：保護組織的技術資產免受環境威脅。
  - **PR.IR-03**：實施機制以達成正常及不利情況下抗故障性的要求事項。
  - **PR.IR-04**：足夠的資源容量以確保維持可用性。

偵測（DE）：發現並分析可能的網路安全攻擊和危害。

- **持續監視 (DE.CM)**：監視資產以發現異常情況、危害指示符及其他潛在不良事件。
  - **DE.CM-01**：監視網路與網路服務以發現潛在的不良事件。
  - **DE.CM-02**：監視實體環境以發現潛在的不良事件。
  - **DE.CM-03**：監視人員活動和技術使用，以發現潛在的不良事件。
  - **DE.CM-06**：監視外部服務提供者的活動和服務，以發現潛在的不良事件。
  - **DE.CM-09**：監視計算硬體與軟體、執行環境及其資料，以發現潛在的不良事件。
- **不良事件分析 (DE.AE)**：分析異常、危害指示符及其他潛在不良事件，以將事件特性化並偵測網路安全事件。
  - **DE.AE-02**：分析潛在不良事件以更理解相關活動。
  - **DE.AE-03**：資訊與多個來源相關。
  - **DE.AE-04**：理解不良事件的估計衝擊及範圍。
  - **DE.AE-06**：向授權人員及工具提供有關不良事件的資訊。
  - **DE.AE-07**：網路威脅情報及其他上下文資訊被整合至分析中。
  - **DE.AE-08**：當不良事件符合定義的事故標準時，宣告為事故。

回應 (RS)：針對偵測之網路安全事件採取行動

- **事故管理 (RS.MA)**：對偵測到的網路安全事故回應進行管理。
  - **RS.MA-01**：當與相關第三方協調宣告事故，就會執行事故回應計畫。
  - **RS.MA-02**：對事故報告進行分類及驗證。
  - **RS.MA-03**：對事故進行分類及定優先排序。
  - **RS.MA-04**：事故依需要進行提報或提高。
  - **RS.MA-05**：應用啟動事故復原準則。

- **事故分析 (RS.AN)**：引導調查以確保有效回應並支援鑑識及恢復活動。
  - **RS.AN-03**：執行分析以決定事故期間發生的情況以及事故的根本原因。
  - **RS.AN-06**：記錄調查期間執行的行動，並保留記錄的完整性及起源。
  - **RS.AN-07**：蒐集事故資料及詮釋資料，並保留其完整性及起源。
  - **RS.AN-08**：估計並驗證事故的影響。
- **事故回應報告及溝通(RS.CO)**：依法律、法規或政策的要求事項與內部及外部利害關係者的協調回應活動。
  - **RS.CO-02**：向內部和外部利害關係者通報事故。
  - **RS.CO-03**：與被指定的內部及外部利害關係者共享資訊。
- **事故緩解(RS.MI)**：執行活動是為了防止事件擴大並減輕其影響程度。
  - **RS.MI-01**：事故獲得控制。
  - **RS.MI-02**：事件已被清除。

RECOVER(RC)：恢復受網路安全事故影響的資產及營運。

- **事故復原計畫執行(RC.RP)**：執行恢復活動以確保受網路安全事故影響的系統及服務的營運可用性。
  - **RC.RP-01**：事故回應計畫的恢復部分於事故回應過程啟動後立即執行。
  - **RC.RP-02**：選擇、決定適用範圍、決定優先排序並執行恢復行動。
  - **RC.RP-03**：在使用備份和其他復原資產進行復原前驗證其完整性。
  - **RC.RP-04**：考量關鍵任務功能與網路安全風險管理，以建立事故後操作的正規化。
  - **RC.RP-05**：驗證恢復資產的完整性，系統及服務的恢復，以確認運作狀態的正常。
  - **RC.RP-06**：依準則宣告事故復原結束，並完成事故相關紀錄。
- **事故復原溝通(RC.CO)**：與內部和外部各方協調恢復活動
  - **RC.CO-03**：將恢復活動及復原營運能力的進展向指定的內部及外部利害關係者傳達。
  - **RC.CO-04**：使用認可的方法及訊息共享事故復原的公共更新。

附錄 B　CSF 層級

表 2 包含第 3 節中討論 CSF 層級之概念性說明。層級是將組織的網路安全風險治理(GOVERN)實踐及網路安全風險管理實踐(識別(IDENTIFY)、保護(PROTECT)、偵測(DETECT)、回應(RESPOND)及復原(RECOVER)) 的嚴格性特徵化。

表 2. CSF 層級的概念性說明

層級	網路安全風險治理	網路安全風險管理
層級 1： 部分	組織網路安全風險策略的應用以臨時方式進行管理。 優先排序是臨時的，並不正式基於目標或威脅環境決定。	組織層面對網路安全風險的認知有限。 組織不定期、逐案實施網路安全風險管理。 組織可能沒有在組織內共享網路安全資訊的過程。 組織通常不理解與其供應者及其獲得及使用的產品與服務，相關的網路安全風險。
層級 2： 風險告知	風險管理實務經管理層認可，但可能不會建立組織範圍內的政策。 網路安全活動及保護需求的優先排序直接由組織風險目標、威脅環境或業務/任務要求事項告知。	組織層面已經具備網路安全風險意識，但尚未建立組織範圍內的網路安全風險管理作法。 組織目標及專案中，針對網路安全的考量可能發生在組織的某些級別，但非所有級別。針對組織和外部資產進行網路風險評鑑，但通常不可重複或不可重複發生。 網路安全資訊在組織內以非正式基礎上分享。

		組織察覺與其提供及使用的產品與服務相關的網路安全風險，但無採取一致或正式行動以回應這些風險。
層級 3：可重複	組織風險管理實務已正式認可並表示為政策。 已知風險政策、過程及程序被定義、依預期實施並審查。 基於風險管理流程對業務/任務的要求事項、威脅及技術全景(landscape)的應用，定期更新組織網路安全實務。	有一種組織範圍內的作法來管理網路安全風險。 網路安全資訊通常在整個組織內共用。 採取一致的方法來有效應對風險變化。人員具有執行其指定角色與職責的知識與技能。 組織一致的、準確地監視資產的網路安全風險。網路安全和非網路安全高階主管定期就網路安全風險進行溝通。高階管理人員確保組織內所有營運部門皆考量網路安全。 組織風險策略由與其提供和使用的產品和服務相關的網路安全風險決定。人員正式對這些風險採取行動，包含藉由書面協議等機制來溝通要求事項、治理結構（例如風險委員會）及政策實施和監視的底線。 這些行動將與預期一致地實施，

		並持續進行監視和審查。
層級 4： 適應性	有一種組織範圍內的作法來管理網路安全風險，係使用已知風險的策略、過程及程序因應潛在性的網路安全事件。在作出決策時清楚地理解並考量網路安全風險與組織目標間的關係。 高階主管在與財務和其他組織風險相同的情境下監視網路安全風險。組織預算是基於對現行及預測的風險環境及風險容忍度的了解。 業務部門在組織風險容忍度的範圍內實施執行願景並分析系統級風險。 網路安全風險管理是組織文化的一部分。源自於對先前活動的認知及對組織系統及網路活動的持續認知。組織可快速且有效地解釋業務/任務目標如何處理及溝通風險方面的變化。	組織依先前與現行的網路安全活動，包含學到的教訓及預估的指標，來調整其網路安全實務。透過合併先進的網路安全技術與實務之持續改良過程，組織可積極適應不斷變化的技術環境，並即時有效地回應不斷變化的複雜威脅。 組織使用即時或近即時資訊以了解與其提供及使用的產品與服務相關的網路安全風險並採取一致的行動。 網路安全資訊在整個組織內將不斷的與第三方授權進行共享。

附錄 C 專用詞彙

CSF 類別

一組與網路安全相關的成果，共同組成 CSF 功能。

CSF 社群剖繪

建立及發布的 CSF 成果基礎線，是為了因應多個組織間的共同利益及目標。社群剖繪通常是針對特定部門、子部門、技術、威脅類型或其他使用案例而開發。 組織可使用社群剖繪作為自己目標剖繪的基礎。

CSF 核心

高階網路安全成果的分類，可協助任何組織管理其網路安全風險。分別由功能、類別及子類別的階層所組成，並詳細說明每個成果。

CSF 現行剖繪

組織剖繪的一部分，指定組織目前正在達成（或企圖達成）的核心成果，並將每個成果的達成方式或程度進行特徵化。

CSF 功能

組織網路安全成果的最高階層。CSF 有六種功能：治理(Govern)、識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond)及復原(Recover)。

CSF 實施示例

一種簡潔、行動導向的概念性說明，協助達成 CSF 核心成果的方式。

CSF 資訊參考

指示 CSF 核心成果與現存標準、指導綱要、法規或其他內容之間的對應關係。

CSF 組織剖繪

依 CSF 核心成果描述組織目前及/或目標網路安全態勢的機制。

CSF 快速入門指引

補充資源用於針對特定的 CSF 相關主題提供簡短、可操作的指引。

CSF 子類別

構成 CSF 類別的技術及管理網路安全活動一組較特定的成果。

CSF 目標剖繪

組織剖繪的一部分，用於指定組織為達成其網路安全風險管理目標而選擇及定優先順序所需的核心成果。

CSF 層級

將組織的網路安全風險治理及管理實踐的嚴格性特徵化。

有四個層級：部分(層級 1)、風險告知(層級 2)、可重複(層級 3)及適應性(層級 4)。

本文件用於識別商業或非商業的設備、儀器、軟體或材料，以充分地規範實驗程序。此識別並不代表著 NIST 建議或對任何產品或服務背書，也不代表著所識別的材料或設備必定對此用途最為可用的。

NIST 技術系列政策

版權、使用及授權聲明

NIST 技術系列出版品識別字語法

如何引用此 NIST 技術系列出版品：

美國國家標準暨技術研究院(2023) NIST 網路安全框架 2.0。(美國國家標準暨技術研究院，馬里蘭州蓋瑟斯堡)，NIST 網路安全白皮書 (CSWP) NIST CSWP 29。

https://doi.org/10.6028/NIST.CSWP.29.chi

聯絡資訊

cyberframework@nist.gov

美國國家標準暨技術研究院

收件者：資訊科技實驗室應用網路安全部

100 Bureau Drive (Mail Stop 2000) 蓋瑟斯堡, MD 20899-2000

所有意見發布均依據《資訊自由法》(FOIA)。