106年

國家資通安全防護整合服務計畫

領域ISAC實務建置指引

(V1.0)

中華民國106年3月

修訂歷史紀錄表

項次	計畫資訊			發行紀錄		說明
	年度	版次	修訂日期	版次	日期	
1	106	V1.0	106/3	V1.0	106/3	新編
2						
3						

資料來源：技服中心整理

目　次

圖 目 次

表 目 次

1. 前言

為了落實推動國家關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)，特制定本領域資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)實務建置指引，作為關鍵基礎設施領域層級與關鍵基礎設施提供者，於執行領域 ISAC 建置與維運的作業參考。領域層級可依循本指引，再根據各領域特性，調整為各領域實務上適用的規範。

1.1. 目的

ISAC 主要任務為透過情資的蒐集、交換及分析，了解各類型資安威脅與弱點資訊，並提供分析結果與對策，針對可能之威脅進行有效預防措施；此外，並與各領域會員進行交流，強化情資分享與協調聯防機制，透過分享資安相關情資與分析報告，以利決策者與資安防護人員有效因應資安事件。

縱觀國際上 ISAC 之發展，首先為美國於 1998 年總統決策指令(Presidential Decision Directive 63, PDD-63)[2]要求政府機關與民間單位應識別與分享其網際網路或實體相關之威脅、弱點及資安事件，以保護國家重要的基礎建設；於 2003 年以國土安全總統指令(Homeland Security Presidential Directive 7, HSPD-7)[3]明確要求資安資訊分享之任務，應涵蓋重要民生基礎建設 ISAC，如金融、電力、能源、運輸及醫療等產業；2013 年總統政策指令(Presidential Policy Directive 21, PPD-21)[4]目標為強化關鍵基礎設施之安全可靠，透過有效的情資交換建立防護陣線，以對抗實體與網路之安全議題。依美國負責跨領域 ISAC 管理之組織 National Council of ISACs(NCI)，現行已涵蓋 24 個產業 ISAC。

我國於民國 90 年成立「行政院國家資通安全會報(以下簡稱資安會報)」，積極推動我國資通安全基礎設施工作；資安會報於民國 97 年起推動跨領域

之資安資訊分享與分析工作，「政府資安資訊分享與分析中心 Government ISAC(G-ISAC)於民國 98 年 11 月正式運作，透過 G-ISAC 之情資分析與分享能力,讓各事業主管機關所設立之ISAC間,能透過會員制度之交流模式，達成資安早期應變與預警效益。透過情資格式標準化與系統自動化之情資分享機制，橫向交流各領域之資安威脅與訊息，達到情資整合、分享及應用之目的，提升國家資訊安全整體應變與防護能力。

如今針對關鍵基礎設施而來的網路攻擊正在增加，經由網路攻擊導致大規模公共服務中斷的想像，其實現之日亦更往前進一步，未來如何迅速掌握各 CI 領域與民間重要產業遭攻擊情資並立即應變，則為政府在整體資安防護方面之重要課題。此外，鑒於國內外資安情資來源漸趨多元，跨領域情資日益增加，需建立更有效之國家層級 ISAC(National ISAC, N-ISAC)運作機制，透過統一之情資格式，利用系統自動分享，提升情資分享內容之即時性、正確性及完整性與自動更新各領域之資安威脅與訊息，達到情資迅速整合、快速分享及有效應用之目的，以提升國家資訊安全整體應變與防護能力。

1.2.適用對象

本指引適用對象為行政院「國家資通安全會報」於網際防護體系下設「關鍵資訊基礎設施安全管理組」，並依 8 大領域區分之主政機關，詳見圖 1。

如有建置領域 ISAC 需求之政府機關(構)或民間企業組織，亦可使用本指引做為建置領域 ISAC 之參考資料。

●8 大領域，共計 7 個主政機關

– 通訊傳播分組，主政機關：通傳會

– 衛生醫療分組，主政機關：衛福部

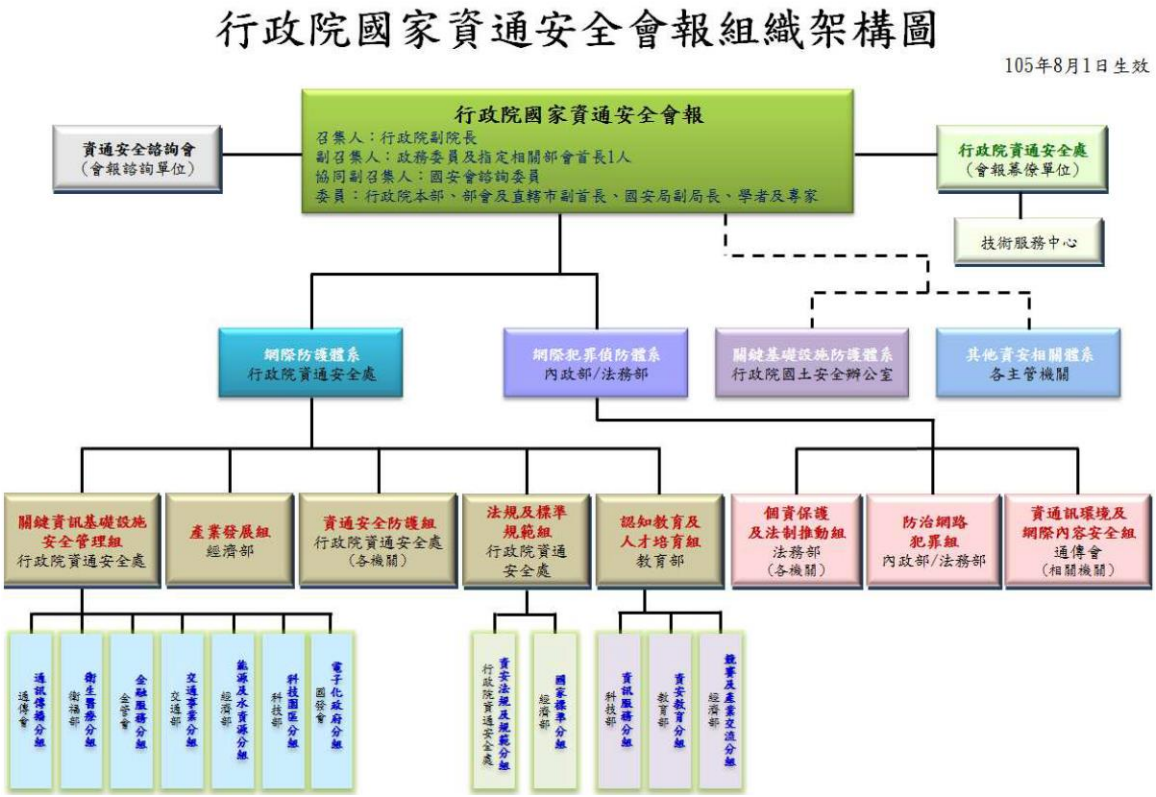
– 金融服務分組，主政機關：金管會

– 交通事業分組，主政機關：交通部

– 能源及水資源分組，主政機關：經濟部

– 科技園區分組，主政機關：科技部

– 電子化政府分組，主政機關：國發會

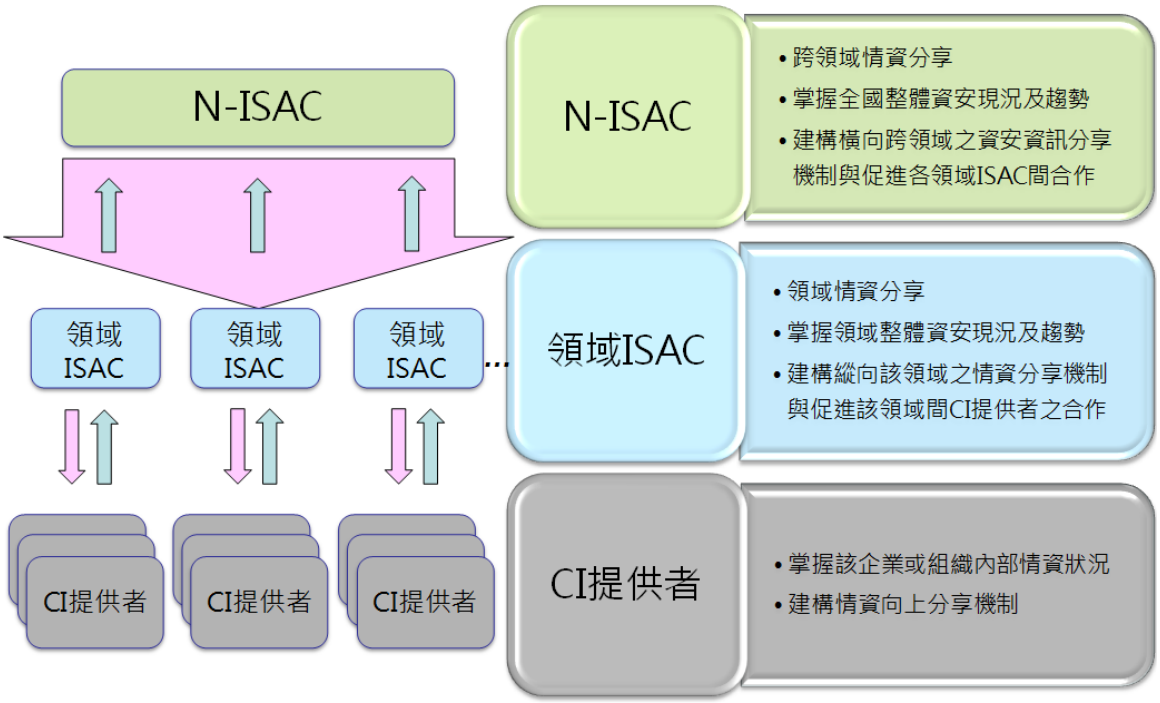


資料來源：行政院國家資通安全會報[5]

圖1　行政院國家資通安全會報組織架構

2. 角色權責與分工

配合我國關鍵資訊基礎設施保護基本政策，其所要求關鍵資訊基礎設施保護原則，規劃 ISAC 體系將分為國家層級(N-ISAC)、各 CI 領域層級(領域 ISAC)及 CI 提供者層級(CI 提供者)等 3 個階層。ISAC 體系角色與分工詳見圖 2。



資料來源：技服中心整理

圖2　角色權責與分工示意圖

2.1.國家層級(N-ISAC)

ISAC 體系中最上層為國家層級之 N-ISAC，其主責為跨領域情資分享，俾利掌握整體資安現況與趨勢，並且透過建構橫向跨領域之資安資訊分享機制，達成與促進各領域 ISAC 間之合作。

2.2.各 CI 領域層級(領域 ISAC)

ISAC 體系中第二層為各 CI 領域層級，角色為各 CI 領域主管機關所維運之領域 ISAC。其主責為 CI 領域內之情資分享，以掌握轄管領域內資安防護現況與趨勢，透過建構縱向之情資分享機制，促進該領域內相關成員之合作。

2.3.各 CI 提供者層級(CI 提供者)

ISAC 體系中第三層為各 CI 提供者層級,角色為各 CI 領域中之 CI 提供者，其責任為掌握自身單位資安現況，適當處理所接收到情資訊息，此外可視資源情況建構情資向上分享機制。

3. 建置實務

本指引將以領域ISAC之建置作業為模型,逐步說明建置ISAC之參考步驟，以 Plan-Do-Check-Act(PDCA)循環之各階段作業項目進行，詳見圖 3。

●規劃階段(Plan)

領域 ISAC 應規劃建置團隊，確認領域 ISAC 之服務項目與內容，並擬定建置計畫。

●執行階段(Do)

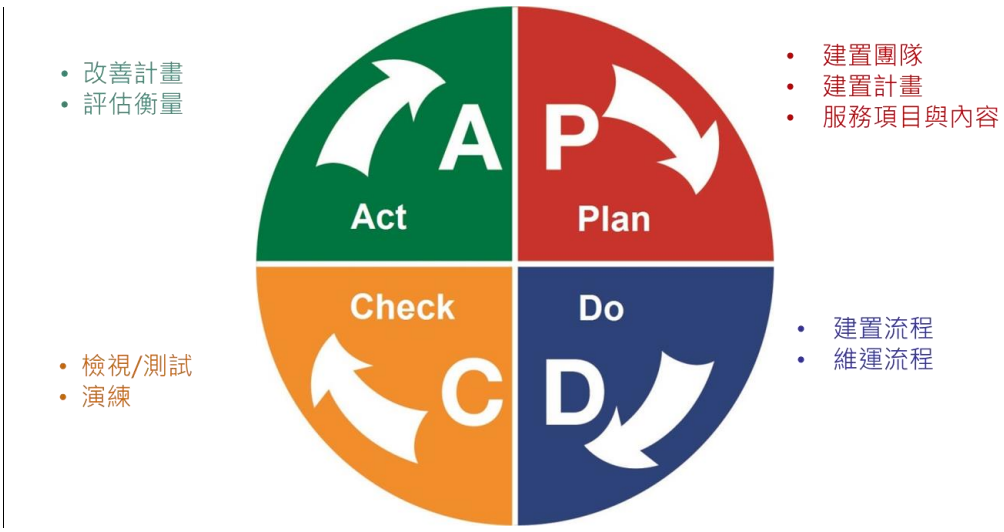
領域 ISAC 應就建置時期與後續維運作業，訂定與實作相關規範與作業程序。

●查核階段(Check)

領域 ISAC 應訂定檢視與測試相關程序，並定期執行。此外，應落實業務項目之演練作業，以利執行人員熟悉相關作業項目與程序。

●改善階段(Act)

領域 ISAC 應規範管理審查機制，確保領域 ISAC 之運作符合預期目標。此外，應依據管理審查內容訂定改善計畫，並落實追蹤。



資料來源：技服中心整理

圖3　PDCA 建置循環

3.1.規劃階段

本節將以領域 ISAC 為適用對象，說明規劃階段所進行之各規劃事項。

3.1.1. 建置團隊

建置領域 ISAC 應組成明確之團隊-，並且併同後續維運工作之需求考量，設計合適之組織架構，其組成可參照 ISAC 建置團隊參考架構，詳見圖 4，建議應包含決策管理組、建置工作組及維運工作組等，分別說明如下：

●決策管理組

決策管理組應由該 CI 領域中之關鍵決策角色負責領導，如資安會報關鍵資訊基礎設施安全管理組各分組之決策管理人員，以確保領域 ISAC 建置與後續維運作業，均符合策略目標與管理要求。

●建置工作組

領域 ISAC 應依照建置計畫需求，籌組適當之建置工作組，規劃人員與工

作項目，以利建置計畫執行，舉例說明如下：

– 專案規劃分組：負責領域 ISAC 建置專案管理，執行需求分析、運作流程規劃及時程管控等。

– 系統開發分組：負責領域 ISAC 情資交換平台開發與系統功能實作，以及發展相關應用程式介面(Application Programming Interface, API)。

●維運工作組

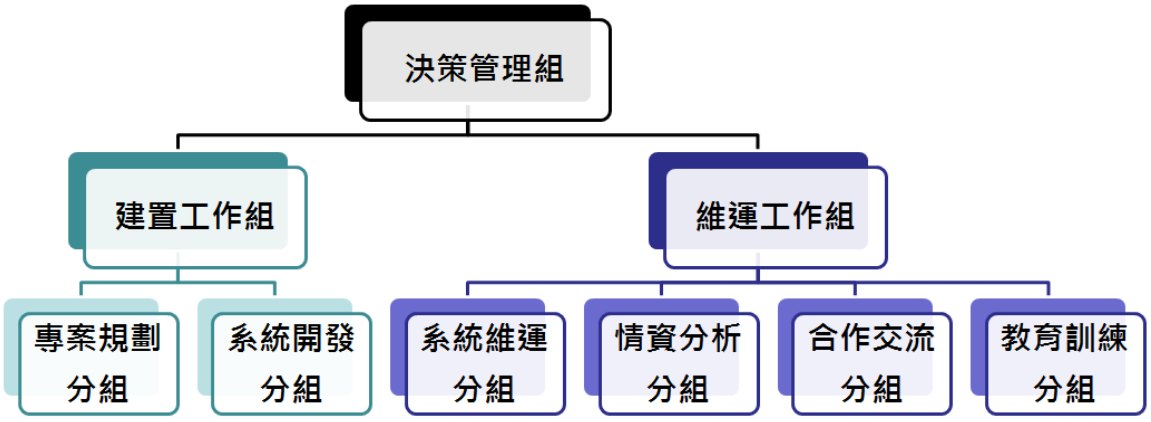
領域 ISAC 建置團隊應依實際規劃之服務項目，籌組適當之維運工作組，舉例說明如下：

– 系統維運分組：負責領域 ISAC 情資交換平台之系統維運相關事項。

– 情資分析分組：負責分析威脅與弱點情資，並研判潛在之資安風險。

– 合作交流分組：負責領域 ISAC 之情資分享與日常作業管理，以及國際交流業務項目。

– 教育訓練分組：負責領域 ISAC 之教育訓練服務項目。



資料來源：技服中心整理

圖4　ISAC 建置團隊參考架構

3.1.2. 建置計畫

建置領域 ISAC 應先進行需求分析，以了解所在 CI 領域之特殊業務與相關情資需求，並識別領域內情資分享範圍與對象，以妥善配置相關資源。

3.1.2.1. 需求分析

●定義 CI 領域內核心業務項目

領域 ISAC 應識別其 CI 領域之核心業務項目，如關鍵資訊基礎設施，落實完成資訊系統分級與資安防護基準作業規定[6]，以釐清 CIIP 範圍。

●識別情資範圍

領域 ISAC 應就所定義之核心業務項目，釐清其所相關之資安威脅、弱點及已知事件等情資需求，如 CI 領域內特有之設備器材、資訊系統及相關應用服務等，以識別情資範圍。

●識別分享對象

領域 ISAC 應明確識別分享服務之對象，以及其情資分享之管道，俾利 CI 領域內之相關產業組織或單位能有效接收與利用情資。

●確認服務項目內容

領域 ISAC 應就服務項目進行評估，如資安情資分享、威脅與弱點分析、國際交流及資安教育訓練等，配合可取得的資源，訂定適宜之 ISAC 服務項目，有關 ISAC 服務項目詳見表 1。

●評估與規劃資源需求

領域ISAC應依據服務項目內容,評估建置與維運作業所需要之資源需求，如人力、經費與時程等，並適當規劃與分配相關資源。

表1　ISAC 服務項目參照列表

項次	服務項目	領域 ISAC 辦理說明
1	資安情資分享	必要項目
2	威脅與弱點分析	必要項目，或與外部組織合作辦理
3	國際交流	可選擇項目
4	資安教育訓練	必要項目，針對 CI 領域辦理訓練
5	緊急情況合作	必要項目
6	資安事件通報	可與其他單位或組織合作辦理(領域 CERT)
7	資安事件協助處理	可與其他單位或組織合作辦理(領域 CERT)
8	資安監控與偵測	可與其他單位或組織合作辦理(領域 SOC)
9	其他	由領域 ISAC 自行評估

資料來源：技服中心整理

3.1.2.2. 建置資源

建置領域 ISAC 應規劃維運之經費來源，例如透過政府編列預算支應、自行籌措經費或採行會員收費等，並妥善訂定經費來源之配置比例。

有關會員收費模式可透過會員分級，以對應不同級距結構之權利與費用，例如美國 FS-ISAC 之會員分級收費資訊，詳見表 2。

表2　ISAC 會員分級收費模式參考列表

會員等級	年費(美金)	會員等級說明
初階會員	$850	總資產價值達 10~100 億；或營收<1 億
標準會員	$5,000	總資產價值達 100~200 億；或營收 1~10 億
進階會員	$10,000	總資產價值達 200~1000 億；或營收 10~25 億

會員等級	年費(美金)	會員等級說明
金級會員	$24,950	總資產價值達 1000~2500 億；或營收 25~50 億
白金會員	$49,950	總資產價值>2500 億；或營收>50 億

資料來源：FS-ISAC[7]

3.1.2.3. 規範與規格

建置領域 ISAC 應配合統一之情資格式與自動系統傳輸架構，明確訂定情資交換平台使用之規格，以及情資交流之相關規範。

●情資交換協定

情資交換平台應配合 N-ISAC 情資交換格式與系統架構，宜採用 Structured Threat Information eXpression(STIX)格式與 Trusted Automated eXchange of Indicator Information(TAXII)傳輸架構，其中情資內容描述宜採用 Cyber Observable eXpression(CybOX)，以利跨組織之情資傳遞與交流。

– STIX

STIX 是一個共同合作開發的標準結構化語言，用於規範、獲取、描述和傳達標準化網路威脅資訊，使用擴展標記語言(Extensible Markup Language, XML)格式進行撰寫，便利於封裝情資資訊，並且具有高度的可解讀性，方便人類與機器進行解讀，同時 XML 也有良好的擴展性，能透過編寫將既有資訊進行擴展。

STIX 情資除了便利封裝，能將情資進行儲存、傳遞、分享與分析，目前美國國土安全部旗下的資通安全辦公室(Office of Cybersecurity and Communications)、國家網路安全和通訊整合中心(National Cybersecurity and Communications Integration Center)及美國電腦緊急應變小組(US-CERT)目前正在使用其架構進行情資分享，也努力推廣架構與相關

技術。

STIX 架構分為 9 大模組，其模組本身或相互之間可具有關聯性與上下關係，模組說明詳見表 3，細節資訊可參考 STIX Project 網站[8]。

表3　STIX 模組列表

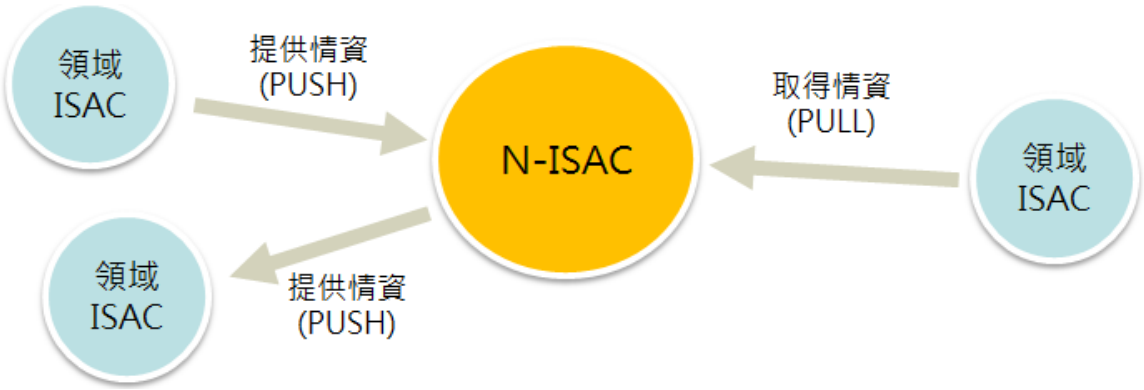
項次	模組名稱	模組說明
1	資安威脅觀察資料 (Observables)	敘述資安威脅事件中所觀察到的相關資料，內容可包含資料來源、資料名稱、內容敘述、資料真實性及相關資安威脅事件等
2	資安威脅模式 (Indicator)	敘述資安威脅可能被觀察到的活動模式，內容可包含威脅模式名稱、模式描述、有效時間、攻擊手法、觀察資料及網際狙殺鍊階段(cyber kill chain)等
3	資安威脅事件 (Incident)	敘述資安威脅事件，內容可包含事件名稱、事件描述、事件類型、受害者、影響範圍與影響資產等
4	資安威脅手法(Tactics, Techniques, and Procedures, TTP)	敘述資安威脅策略、技術與手法，內容可包含資安漏洞、攻擊模式、惡意程式、使用工具、受害者及網際攻擊狙殺鍊階段等
5	資安威脅活動 (Campaign)	敘述資安威脅活動資訊，內容可包含一群駭客、攻擊手法、威脅模式與相關事件，甚至可推演關聯至其他相關資安威脅活動
6	資安威脅者(Threat Actors)	敘述資安威脅者的特徵與描述資訊，內容可包含相關基本描述、資安威脅活動、威脅手法、情資來源及動機等
7	資安威脅目標(Exploit Target)	敘述被惡意利用的資安漏洞、弱點及設定檔，內容可包含目標名稱、目標描述、資安漏洞、資安弱點、因應措施、處理狀況及相

項次	模組名稱	模組說明
		關資安威脅手法等
8	資安威脅防護措施(Course of Action)	敘述面對資安威脅所做的應變與預防措施，內容可包含防護措施名稱、描述、效用、使用成本、應用範圍及相關防護措施等
9	資安威脅報告(Reports)	綜整各模組資訊而成資安威脅報告，也可處理難以單一套用至其他模組的資安資訊，設計此模組以文字格式彈性封裝資安資訊

資料來源：技服中心整理

– TAXII

TAXII 是一套網路威脅情資交換傳輸機制，其功能為提供組織與合作夥伴傳遞與共享情資。TAXII 服務功能包含接收服務(Inbox Service)、收取服務(Poll Service)、探索服務(Discovery Service)及訂閱管理(Collection Management Service)，透過上述服務功能之運作，TAXII 可支援軸輻型、訂閱型及點對點等 3 種情資分享模型，目前我國 N-ISAC 採用軸輻型情資分享模型，詳見圖 5，以利情資管理與交流。



資料來源：技服中心整理

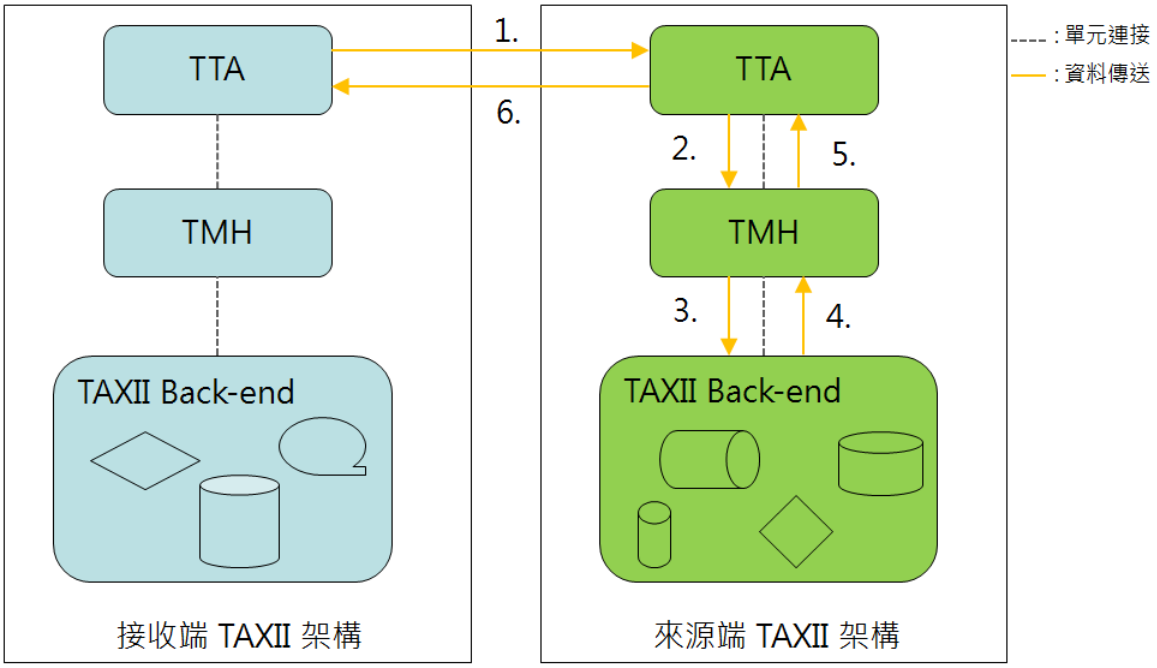
圖5　N-ISAC 情資分享模型架構

TAXII 之功能模組包含網路連接、訊息處理及後端管理等功能單元，相關功能單元說明與運作架構詳見表 4 與圖 6，細節資訊可參考 TAXII Project 網站[9]。

表4　TAXII 功能單元列表

功能單元	說明
網路連接單元 TAXII Transfer Agent (TTA)	▪ 負責傳送/接收 TAXII 訊息 ▪ 透過網路與其他 TTA 通訊，處理協定需求的細節 ▪ 不處理 TAXII 訊息內容(由 TMH 處理)
訊息處理單元 TAXII Message Handler (TMH)	▪ 負責產生/解讀 TAXII 訊息，解析 TTA 收到的 TAXII 訊息，或建構一個可傳送的 TAXII 訊息 ▪ 與 TAXII Back-end 連接，將來自 Back-end 的訊息轉換為 TAXII 訊息，或基於 TTA 接收的 TAXII 訊息執行動作
後端單元 TAXII Back-end	後端單元，負責資料儲存、訂閱管理、存取控制決定、內容過濾及其他活動

資料來源：技服中心整理



資料來源：TAXII Project 網站[9]

圖6　TAXII 功能單元運作架構

– CybOX

CybOX 是一個標準化的方法(schema)，用以編碼和傳達高精確度的結構化語言，描述所有可以從電腦系統和操作上觀測到的事件內容、行為或狀態特性，CybOX 可支援下列網路安全領域，細節資訊可參考 CybOX Project 網站[10]。

➢威脅評估與描述 (Threat assessment and characterization)

➢惡意軟體描述 (Malware characterization)

➢操作事件管理 (Operational event management)

➢安全性資訊與事件管理/記錄 (Security information and event management/Logging)

➢網路情境感知 (Cyber situational awareness)

➢事件應變 (Incident response)

➢指標共享 (Indicator sharing)

➢數位鑑識 (Digital forensics)

●情資格式規範

– 情資類型

情資類型可參考 N-ISAC 所規劃之情資類型，情資類型詳見表 5。

表5 ISAC 情資類型列表

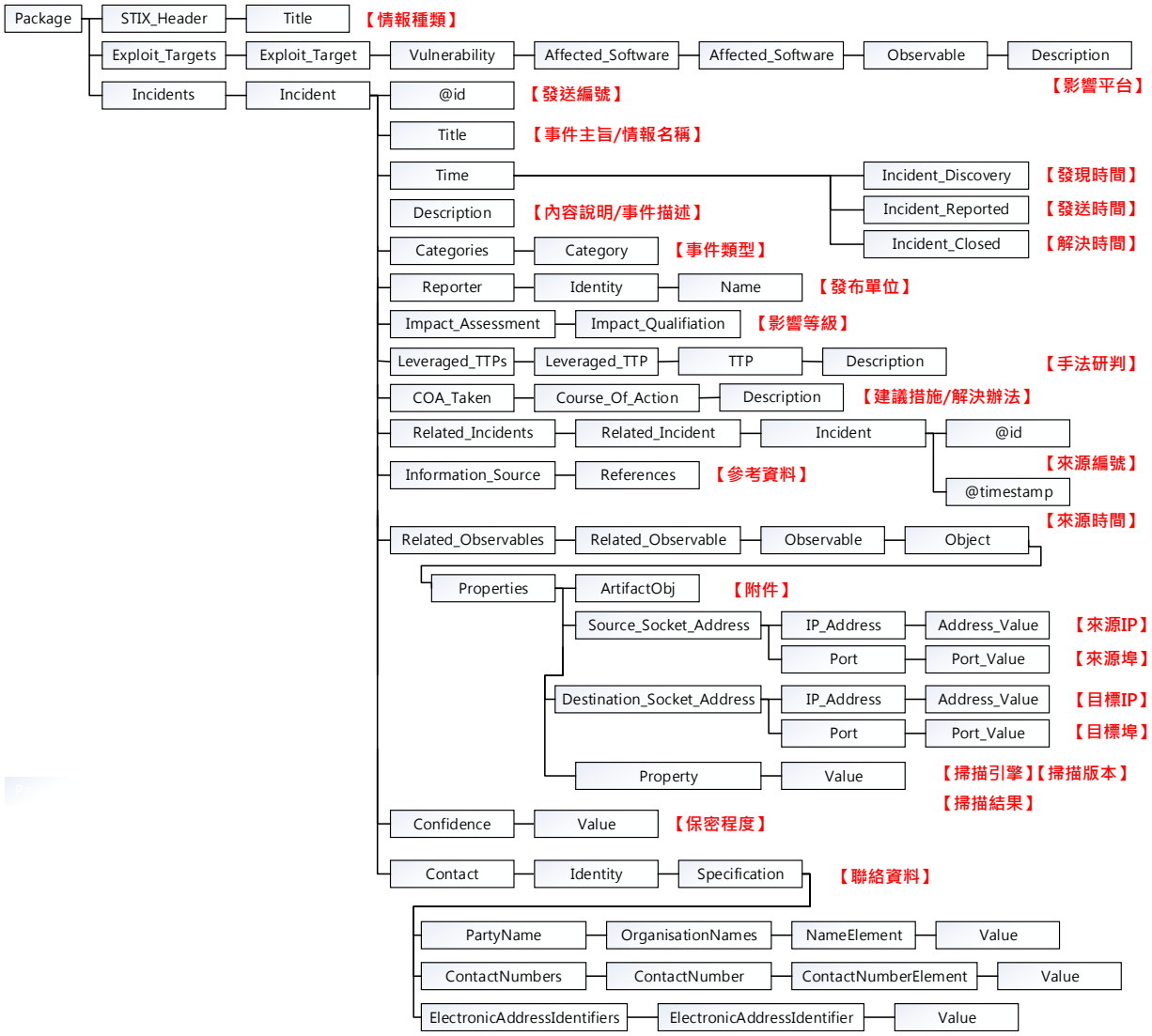
情資類型	內容說明
資安訊息情資(ANA)	▪重大威脅指標情資 ▪資安威脅漏洞與攻擊手法情資 ▪重大資安事件分析報告 ▪資安相關技術或議題之經驗分享
資安預警情資(EWA)	▪疑似存在系統弱點或可疑程式 ▪疑似進行惡意或攻擊行為 ▪進行可疑連線行為或活動
網頁攻擊情資(DEF)	▪特定網頁遭受攻擊且證據明確 ▪特定網頁內容不當且證據明確 ▪特定網頁發生個資外洩且證據明確
入侵攻擊情資(INT)	▪特定系統遭受入侵且證據明確 ▪特定系統進行網路攻擊活動且證據明確
回饋情資(FBI)	▪情資使用或處理情形回饋 ▪分享資安事件統計資料

情資類型	內容說明
	▪情資勘誤資訊回饋

資料來源：技服中心整理

– 情資格式

情資格式可參考 N-ISAC 所規劃之情資格式，情資格式架構詳見圖 7。



資料來源：技服中心整理

圖7　STIX 情資格式架構

●情資交換平台開發架構

領域 ISAC 所建置之情資交換平台，應可自行進行情資管理，並可透過 TAXII 與 N-ISAC 自動進行情資交換，系統架構可參照領域 ISAC 情資交換平台架構，詳見圖 8。

– 情資管理

情資交換平台應包含情資查詢、新增、編輯、刪除、擷取、上傳及統計等管理功能。

– TAXII 情資交換

情資交換平台應實作 TAXII 使用者端 API(Client)，用以介接 N-ISAC 之 TAXII 伺服器端 API(Server)，達成情資自動傳遞之功能。此外，領域 ISAC 如需透過情資交換平台介接其他外部組織或機構，則可視需求自行開發 TAXII 伺服器端 API(Server)。

– 網頁使用者介面(Web User Interface, Web UI)

情資交換平台之 Web UI 應包含使用者操作、身分驗證與權限管理及後端管理等功能模組。

➢使用者操作模組

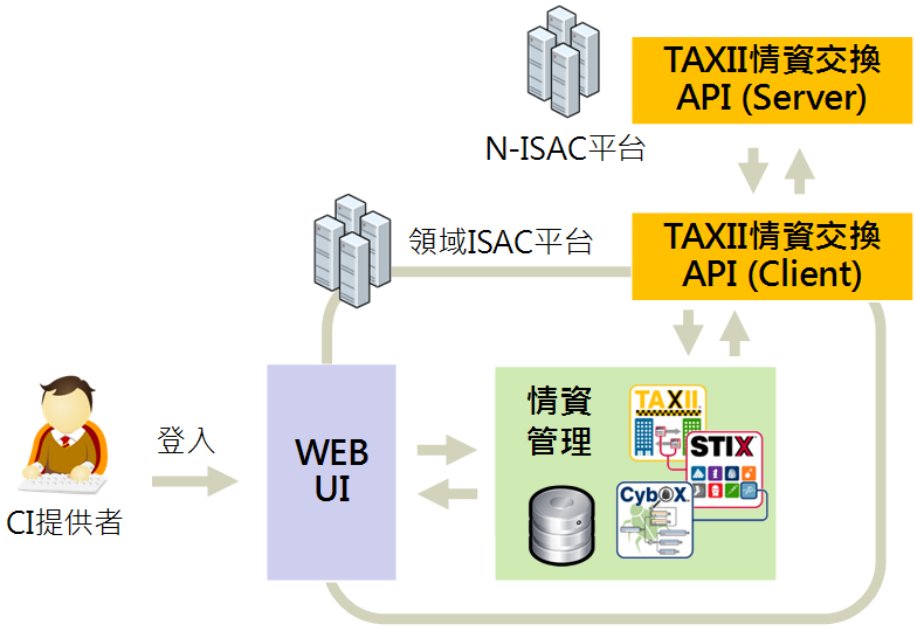
情資交換平台之使用者為領域 ISAC 管理人員，以及其 CI 領域之 CI 提供者，應依各類型使用者之操作需求，建置合適之網頁介面。

➢身分驗證與權限管理模組

情資交換平台應依實際使用需求，設計各類型使用者權限群組，以規範其情資存取或編輯之範圍，並實作身分與權限驗證機制。

➢後端管理模組

情資交換平台應依各項系統服務功能實作管理介面，以供領域 ISAC 管理人員進行設定與管控。



資料來源：技服中心整理

圖8　領域 ISAC 情資交換平台架構圖

●情資交換平台維運安全

– 系統開發安全

情資交換平台之開發應遵循安全軟體發展生命週期(Secure Software Development Life Cycle, SSDLC)，並將資安防護需求與相關安全議題納入評估考量。

– 身分驗證與存取管控

情資交換平台應妥善規劃其帳號管理與身分識別機制，並考量存取系統資料之機密性與安全性。如 CI 領域內已有普遍使用之身分識別機制，如晶片卡或數位憑證等，亦可整合成為情資交換平台之身分驗證功能。

– 委外管理

情資交換平台如有委外開發或維護等情形，相關作業均應訂定資安管理要求與管控措施，以落實委外安全管理。

3.1.2.4. 建置前準備

建置領域 ISAC 應完成擬訂建置計畫，包含作業項目細部執行內容，並訂定各階段里程碑。

3.1.3. 服務項目與內容

建置領域 ISAC 應妥善規劃服務項目與執行內容，並訂定可行之服務目標，有關 ISAC 服務項目之內容詳見表 6。

表6　ISAC 服務項目說明參照列表

項次	服務項目	執行內容	服務目標
1	資安情資分享	▪建置情資交換平台，收接威脅、弱點或事件情資資訊 ▪設置資安情資諮詢服務	情資交換平台可用率達 XX%
2	威脅與弱點分析	▪建立威脅與弱點分析之作業程序 ▪研究資安議題或 CI 領域特定安全議題 ▪CI 領域核心業務項目之相關資安議題，進行情資蒐集、識別及分析潛在風險，定期產出 CI 領域資安威脅分析報告	▪威脅與弱點分析案例達X件 ▪資安議題研究 X 件 ▪CI 領域資安威脅分析報告 X 份
3	國際交流	接收與彙整國際情資，或介接國外相關領域 ISAC	國際情資交流達 X 件
4	資安教育訓練	▪辦理情資交流研討會議，分享相關安全防護議題	▪辦理 XX 人次教育訓練

項次	服務項目	執行內容	服務目標
		▪針對 CI 領域定期辦理資安相關教育訓練，提升資訊安全意識	▪課後測驗通過率達 XX%
5	緊急情況合作	如遇緊急資安事件情況時及時通知 ISAC 成員，並與相關單位(領域 CERT)合作辦理	N/A
6	資安事件通報	協助相關單位(領域 CERT)執行通報業務	N/A
7	資安事件協助處理	協助相關單位(領域 CERT)執行事件處理	N/A
8	資安監控與偵測	協助相關單位(領域 SOC)執行資安監控	N/A
9	其他	由領域 ISAC 自行訂定	自訂目標

資料來源：技服中心整理

3.2.執行階段

本節將以領域 ISAC 為適用對象，說明執行階段所進行之各維運執行事項。

3.2.1. 建置流程

建置領域 ISAC 應依建置計畫進行，建置流程應包含建置計畫擬訂、ISAC 平台建置、ISAC 平台測試及 ISAC 平台上線等程序，詳見圖 9。

●建置計畫擬訂

領域 ISAC 應參考本指引 3.1 節所敘明內容，進行需求分析、評估建置資源及訂定規範與規格，並依需求分析結果，擬訂領域 ISAC 組織架構與相關工作要點。

●ISAC 平台建置

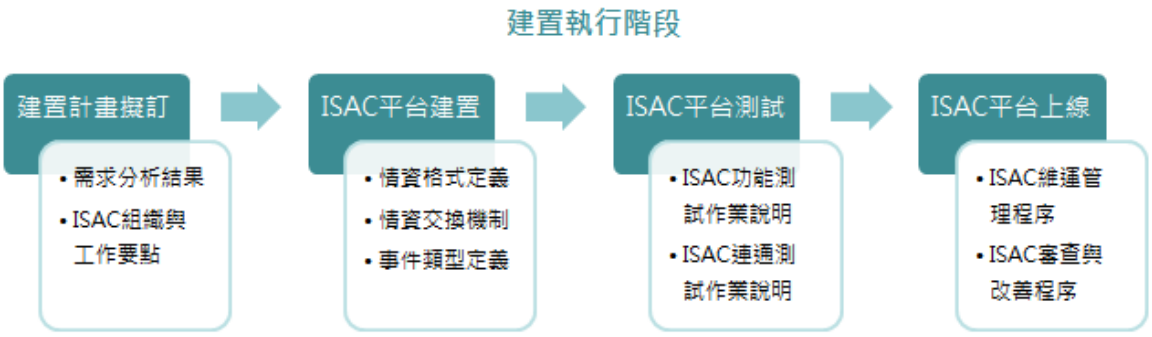
領域 ISAC 應依建置計畫開發 ISAC 情資交換平台，並實作情資交換機制。

●ISAC 平台測試

領域 ISAC 應於 ISAC 情資交換平台上線前，落實執行系統元件測試、系統功能測試、壓力測試及源碼檢測等相關資安檢測作業。

●ISAC 平台上線

領域 ISAC 應就日常維運作業訂定相關管理規範與作業程序，此外為實踐 PDCA 循環，亦應落實執行定期審查與持續改善之管理程序。



資料來源：技服中心整理

圖9　領域 ISAC 建置流程圖

●情資交換平台建置注意事項

– 建立安全可靠的系統環境，供情資管理、儲存、接收及發布

– 落實會員帳號管理、身分驗證及存取控制

– 保護涉及機敏或個人資料之檔案，並對相關資料欄位採適當之遮蔽

– 系統與資料應有妥善之備援機制

– 定期針對系統與相關作業程序，辦理資安內部稽核或外部稽核

– 如有委外之情形，亦需注意委外服務管理與相關安全要求

●ISAC 管理文件

領域 ISAC 應訂定維運 ISAC 所需之相關程序與文件，ISAC 管理相關文件詳見表 7。

表7　ISAC 管理文件參考列表

項次	文件類型	文件內容
1	領域 ISAC 管理政策/規章	▪領域 ISAC 管理規範內容 ▪領域 ISAC 會員申請與核定規範
2	ISAC 組織與工作要點	依建置計畫規劃人員配置，並對照服務項目與內容訂定工作項目，區分角色責任與權限
3	ISAC 維運管理程序	▪情資格式定義、情資交換機制、事件類型定義等規格文件 ▪ISAC 功能測試作業說明、ISAC 連通測試作業說明 ▪ISAC 運作程序
4	ISAC 審查與改善程序	▪ISAC 運作情形量測、評估及分析 ▪定期進行管理審查會議 ▪執行改善計畫與追蹤複核

資料來源：技服中心整理

3.2.2. 維運流程

建置領域 ISAC 應遵循相關作業程序與文件，以落實日常之維運管理。

●ISAC 會員申請與核定作業

領域 ISAC 應建立該 CI 領域之 ISAC 會員申請管道，並定期辦理 ISAC 會

員申請資格審核，落實篩選適宜之 CI 提供者加入領域 ISAC，以創建安全與可信任的情資分享環境。

●情資交換平台維運作業

領域ISAC應確保情資交換平台之實體與環境安全、運作安全及通訊安全，情資交換平台維運作業之相關項目詳見表 8。

表8　情資交換平台維運作業項目參考列表

類型	項目內容
實體與環境安全	實體區域安全、設備安全等
運作安全	變更管理、容量管理、備份管理、日誌管理、軟體管控及更新等
通訊安全	網路安全管控、資訊傳送保護等

資料來源：技服中心整理

●情資交換

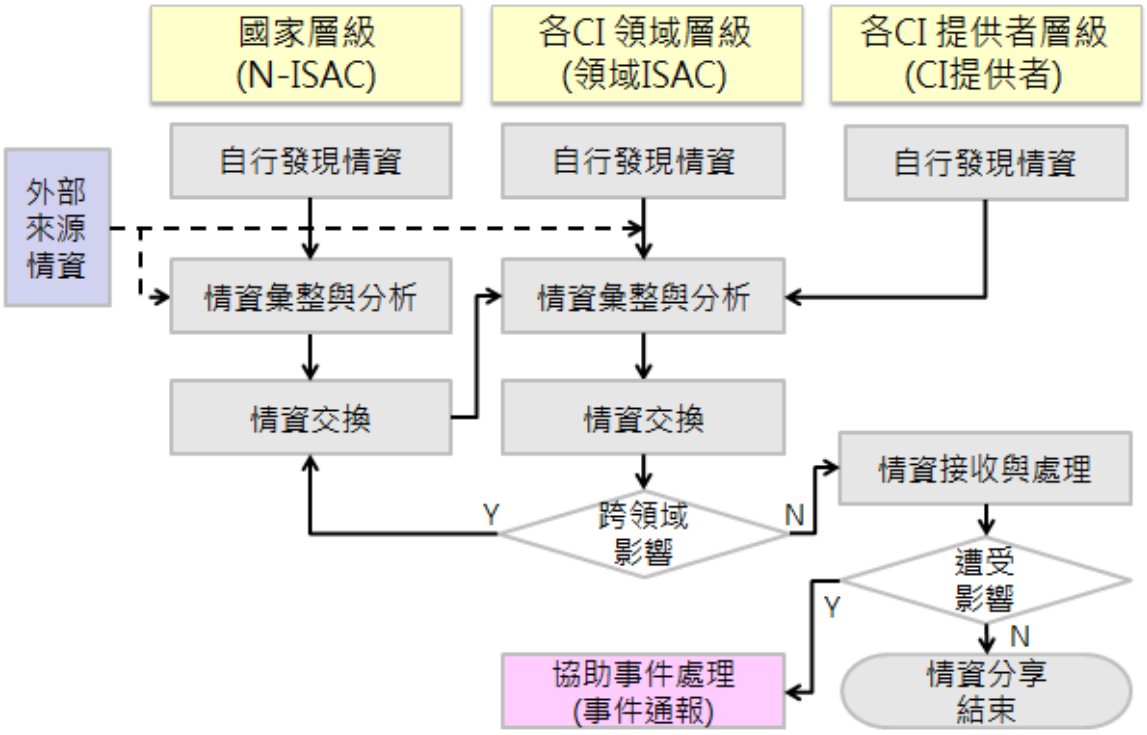
領域 ISAC 應向 N-ISAC 與 CI 提供者進行情資交換，亦可透過 N-ISAC 向其他領域 ISAC 進行跨 CI 領域情資交換，情資交換流程詳見圖 10。

– CI 領域層級向上互動

跨領域或重要威脅、弱點或事件等情資，應由領域 ISAC 將情資分享至 N-ISAC，以利 N-ISAC 掌握整體資安現況與趨勢，建構橫向跨領域之資安資訊分享機制。

– CI 領域層級向下互動

接收各式情資，經彙整與分析情資後分享予 ISAC 會員(CI 提供者)；或於必要時協助 CI 提供者之事件處理。



資料來源：技服中心整理

圖10 ISAC 情資交換流程圖

●與 CERT、SOC 組織互動

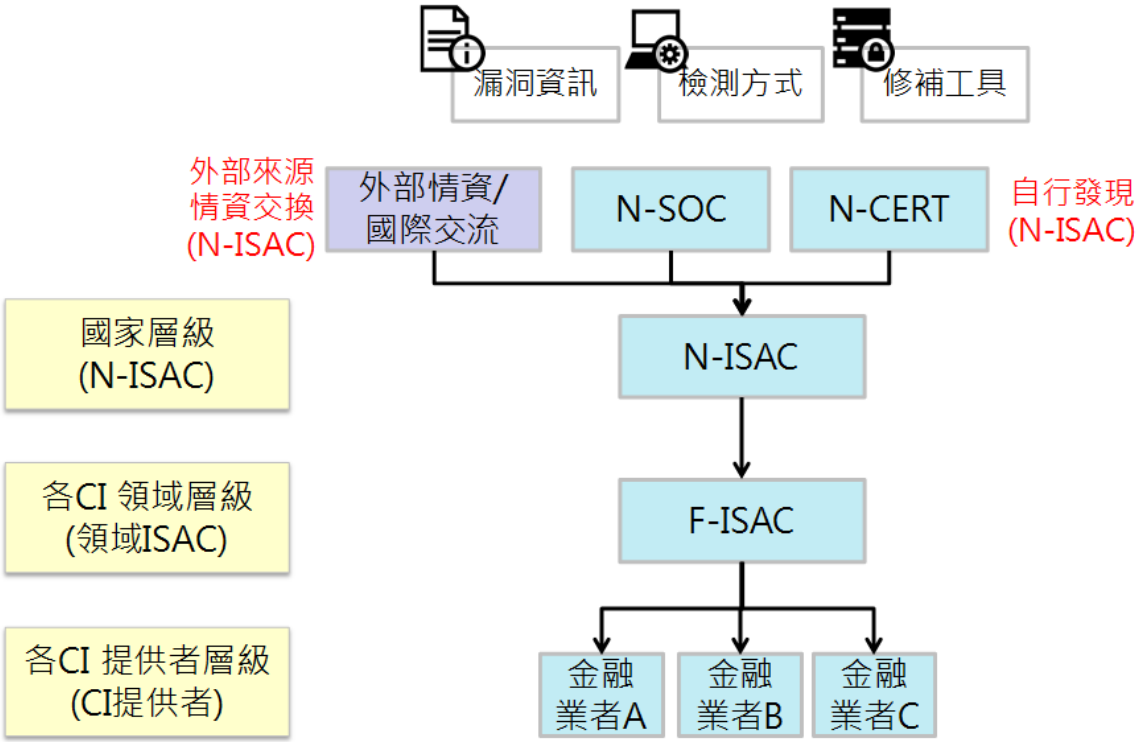
領域 ISAC 應與其 CI 領域之 CERT 與 SOC 組織，進行資安情資、事件通報及監控紀錄之交流互動，以利關鍵資訊基礎設施保護之整體運作。

3.2.3. 應用情境

領域 ISAC 可參考下列之應用情境範例說明，以了解情資交換之運作模式與流程。

●N-ISAC 情資交換

以 N-ISAC、F-ISAC、及金融業者為例說明，詳見圖 11。



資料來源：技服中心整理

圖11 N-ISAC 情資交換情境說明流程圖

– 由 N-ISAC 透過 N-CERT 或 N-SOC 之聯繫，自行發現漏洞資訊，並取得漏洞相關檢測方式或修補工具

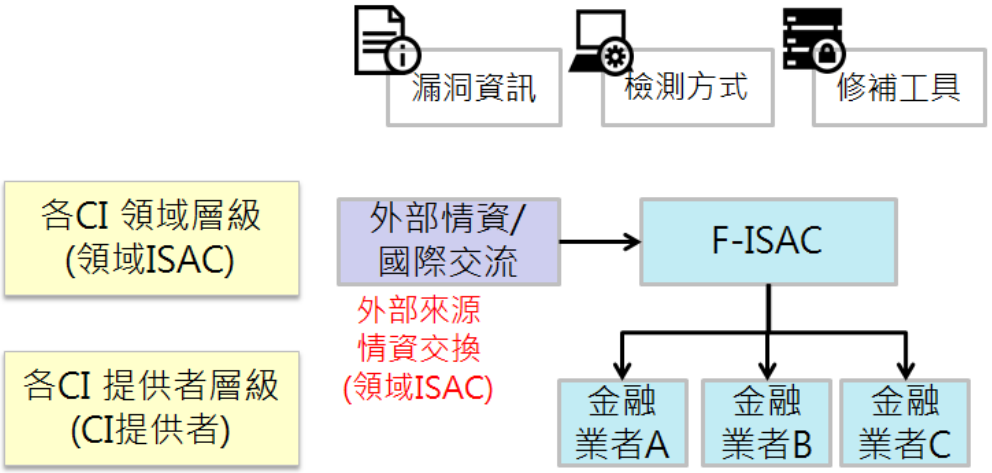
– 由 N-ISAC 取得外部來源情資所提供之漏洞資訊，並取得漏洞相關檢測方式或修補工具

– N-ISAC 將漏洞資訊、檢測方式及修補工具等情資彙整，並提供 F-ISAC(領域 ISAC)

– F-ISAC 將情資提供給相關金融業者(CI 提供者)

●領域 ISAC 情資交換

以 F-ISAC 與金融業者為例說明，詳見圖 12。



資料來源：技服中心整理

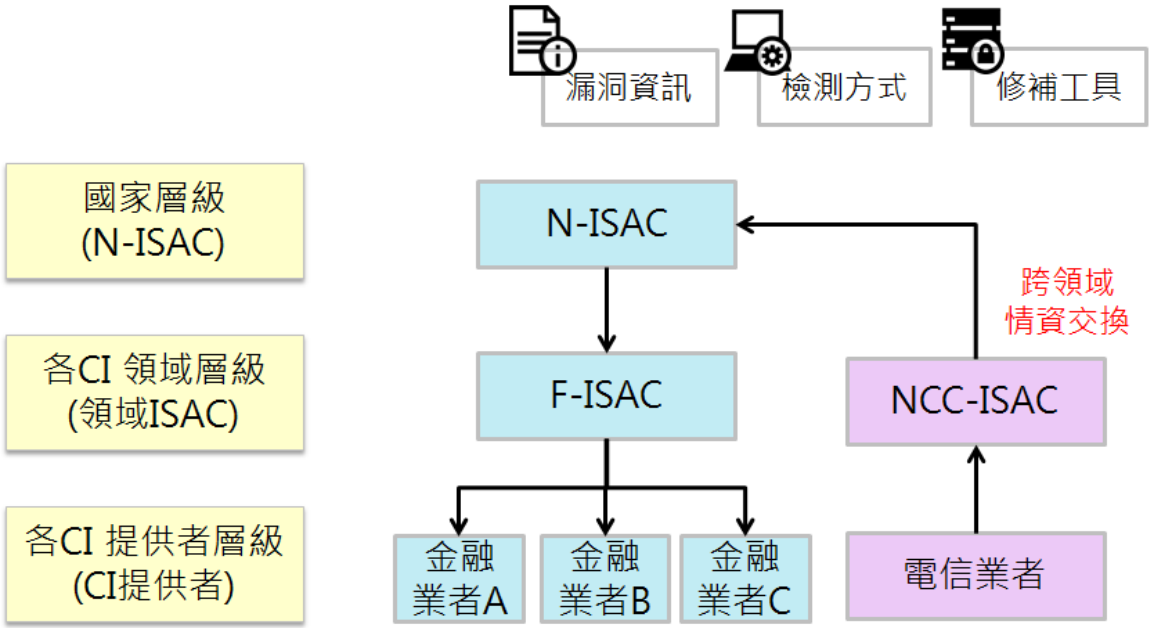
圖12 領域 ISAC 情資交換情境說明流程圖

– 由 F-ISAC(領域 ISAC)取得外部來源情資所提供之漏洞資訊，並取得漏洞相關檢測方式或修補工具

– F-ISAC(領域 ISAC) 將漏洞資訊、檢測方式及修補工具等情資彙整，並提供給相關金融業者(CI 提供者)

●跨領域情資交換

以 N-ISAC、NCC-ISAC、F-ISAC 及金融業者為例說明，詳見圖 13。



資料來源：技服中心整理

圖13 跨領域情資交換情境說明流程圖

– 由電信業者自行發現漏洞資訊，並向上通知 NCC-ISAC

– 由 NCC-ISAC 取得漏洞相關檢測方式或修補工具，並進行情資彙整

– NCC-ISAC 透過 N-ISAC 進行跨領域情資交換，將漏洞資訊、檢測方式及修補工具等情資提供 F-ISAC(領域 ISAC)

– F-ISAC 將情資提供給相關金融業者(CI 提供者)

3.3.查核階段

本節將以領域 ISAC 為適用對象，說明查核階段所進行之各查核事項。

3.3.1. 檢視/測試

●執行情形統計

領域 ISAC 應定期統計情資交換紀錄及彙整領域 ISAC 運作情形，並提報

管理審查。

●定期功能測試

領域 ISAC 建置後應定期檢視或測試下列項目與內容，作為後續改善的依據：

– 身分驗證機制

– 傳輸格式與傳輸安全機制

– 情資分享機制

– 流量壓力測試

3.3.2. 演練

●演練目標

領域 ISAC 應定期辦理情資分享演練，確認情資交換管道順暢運行。

●演練項目

領域 ISAC 執行情資分享演練之內容，應包含領域內或與跨領域之情資交換作業。

3.4.改善階段

本節將以領域 ISAC 為適用對象，說明改善階段所進行之各作業事項。

3.4.1. 改善計畫

領域 ISAC 應依據管理審查之結果，訂定改善計畫，並落實執行追蹤複核。

3.4.2. 評估衡量

●管理審查會議

決策管理組應每年定期召開管理審查會議，審查領域 ISAC 之年度執行情形，以了解情資交換統計資訊、演練執行結果及各式議題，並決議領域 ISAC 之後續執行目標，以確保符合策略目標與管理要求。

●定期追蹤

決策管理組應指派特定人員定期追蹤改善項目，並落實回報權責管理人員，以符合 PDCA 循環之精神。

4. 結論

領域 ISAC 於建置與營運期間，可能遭遇許多原先規劃時未能預料之問題，領域 ISAC 建置團隊必須持續蒐集相關問題以精進情資分享機制與架構。

此外，領域 ISAC 需與所有 ISAC 會員進行有效率的溝通，如定期召開會議或進行問卷調查以取得意見反饋，以持續改善分享機制與架構，達成有效益及效率之情資分享的終極目標。

5. 參考文獻

[1]行政院資通安全處(民 106 年 2 月)。「106 年國家資通安全防護整合服務計畫」需求說明書。未出版。

[2]Presidential Decision Directive 63(1998)

[3]Homeland Security Presidential Directive 7(2003)

[4]Presidential Policy Directive 21(2013)

[5]組織架構(民 105 年 8 月 1 日)。行政院國家資通安全會報。民 106 年 3 月 7 日，取自：https://www.nicst.ey.gov.tw/。

[6]行政院國家資通安全會報(民 104 年 7 月)。資訊系統分級與資安防護基準作業規定。民 104 年 7 月 29 日。

[7]Membership Guidelines by the Financial Services Information Sharing and Analysis Center(n.d.). Financial Services Information Sharing and Analysis Center. Retrieved March 7, 2017, from the World Wide Web: https://www.fsisac.com/

[8]STIX Project by the MITRE Corporation(2017). The MITRE Corporation. Retrieved March 7, 2017, from the World Wide Web: https://stixproject.github.io/

[9]TAXII Project by the MITRE Corporation(2017). The MITRE Corporation. Retrieved March 7, 2017, from the World Wide Web: https://taxiiproject.github.io/

[10]CybOX Project by the MITRE Corporation(2017). The MITRE Corporation. Retrieved March 7, 2017, from the World Wide Web: https://cyboxproject.github.io/

6. 附件

附件 1 國際 ISAC 參考資訊

附件 2 領域 ISAC 建置項目檢核表

附件 3 系統安全需求項目查檢表

附件 4 STIX 情資格式架構

附件1 國際 ISAC 參考資訊

項次	國際 ISAC 名稱 (網址)	CI 領域分類
1	AUTOMOTIVE ISAC https://www.automotiveisac.com/	交通
2	AVIATION ISAC http://www.a-isac.com/	交通
3	FINANCIAL SERVICES ISAC http://www.fsisac.com/	金融
4	Finanicls ISAC Japan http://www.f-isac.jp/	金融
5	NATIONAL HEALTH ISAC http://www.nhisac.org/	醫療
6	ELECTRICITY ISAC http://www.eisac.com/	能源
7	DOWNSTREAM NATURAL GAS ISAC http://www.dngisac.com/	能源
8	EE-ISAC: European Energy http://www.ee-isac.eu/	能源
9	WATER ISAC http://www.waterisac.org/	水資源
10	INFORMATION TECHNOLOGY ISAC https://www.it-isac.org/	資通訊

附件2 領域 ISAC 建置項目檢核表

項次	檢核項目	檢核欄
1	**建置團隊**	
1-1	成立決策管理組，並由決策管理人員擔任召集人	召集人:_____
1-2	規劃區分建置工作組與維運工作組，並指定相關負責人員	工作分組說明:
2	**建置計畫**	
2-1	訂定 ISAC 服務項目內容 1.資安情資分享 (必要項目) 2.威脅與弱點分析 (必要項目) 3.國際交流 (可選擇項目) 4.資安教育訓練 (必要項目) 5.緊急情況合作 (必要項目) 6.資安事件通報 (可與領域 CERT 合作) 7.資安事件協助處理 (可與領域 CERT 合作) 8.資安監控與偵測 (可與領域 SOC 合作) 9.其他	▪□是□否規劃國際交流 ▪□是□否併同建置領域 CERT ▪□是□否併同建置領域 SOC ▪其他說明:
2-2	規劃維運經費來源	▪政府預算:___% ▪自籌款項:___% ▪會員收費:___%
3	**情資交換平台**	
3-1	規劃情資交換平台開發時程	時程說明:
3-2	系統開發是否將資安相關議題納入考量? 1.開發作業安全(SSDLC) 2.身分驗證與存取管控	

項次	檢核項目	檢核欄
4	**維運管理**	
4-1	訂定相關管理文件與作業程序書 1.領域歸 ISAC 管理政策/規章 2.ISAC 組織與工作要點 3.ISAC 維運管理程序 4.ISAC 審查與改善程序	管理文件說明:
4-2	訂定會員申請與核定作業規範	
4-3	情資交換平台是否將安控措施納入維運考量? 1.實體與環境安全 2.運作安全 3.通訊安全	
4-4	訂定委外服務管理程序與相關安全要求	
5	**管理審查**	
5-1	訂定管理審查相關規範	
5-2	訂定改善項目定期追蹤之作業程序	
5-3	訂定演練目標與執行項目	

附件3 系統安全需求項目查檢表

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
機密性	1.1 機敏資料傳輸時，採用加密機制	V	V	V	通用
	1.2 使用公開、國際機構驗證且未遭破解的演算法		V	V	通用
	1.3 使用演算法支援的最大長度金鑰		V	V	通用
	1.4 加密金鑰或憑證週期性更換		V	V	通用
	1.5 加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制			V	通用
	1.6 機敏資料儲存時，採用加密機制			V	通用
完整性	2.1 於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性	V	V	V	通用
	2.2 針對開放下載的資料，也提供資料之雜湊值(HASH Value)供使用者比對其完整性		V	V	通用
	2.3 具有防範 SQL 命令注入攻擊(SQL Injection)之措施		V	V	通用
	2.4 具有防範跨站腳本攻擊(Cross-Site Scripting)之措施		V	V	WEB
	2.5 驗證網頁重導(Redirects)與導向(Forwards)之目的地在合法名單內		V	V	WEB
	2.6 重要系統資料或紀錄留存雜湊值以確保完整性			V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
可用性	3.1 重要資料定時同步至備份或備援環境，並加以保護限制存取	V	V	V	通用
	3.2 採用「高可用性」(High Availability) 架構(分散式或叢集伺服器架構)			V	通用
身分驗證	4.1 除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取	V	V	V	通用
	4.2 身分驗證機制位於伺服器端且採用集中過濾機制(例如使用 Filter 過濾器)		V	V	通用
	4.3 身分驗證相關資訊(帳號、密碼等)不留存於程式原始碼中		V	V	通用
	4.4 確實規範使用者密碼強度 (密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元)		V	V	通用
	4.5 使用者必須定期更換密碼，且至少不可以與前 5 次使用過之密碼相同		V	V	通用
	4.6 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 30 分鐘內不允許該帳號及來源 IP 繼續嘗試登入			V	通用
	4.7 身分驗證相關資訊不以明文傳輸			V	通用
	4.8 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼			V	通用
	4.9 採用圖形驗證碼(CAPTCHA)機制於身分驗證及重要交易行為，以防範自動化程式之嘗試			V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
	4.10重要交易行為要求使用者再次進行身分驗證			V	通用
	4.11採用多重因素身分驗證(兩種以上驗證類型)			V	通用
	4.12密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作			V	通用
授權與存取控制	5.1 執行功能及存取資源前，檢查使用者授權	V	V	V	通用
	5.2 採用伺服端的集中過濾機制檢查使用者授權		V	V	通用
	5.3 對使用者/角色，僅賦予所需要的最低權限		V	V	通用
	5.4 軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行			V	通用
	5.5 除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表(ACL)			V	通用
	5.6 重要行為由多人/角色授權後才得以進行			V	通用
	5.7 具有防範「跨站請求偽造」(Cross-Site Request Forgery，CSRF)攻擊之措施			V	WEB
日誌紀	6.1 針對身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤	V	V	V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
錄	及管理者行為進行日誌記錄				
	6.2 日誌紀錄包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述	V	V	V	通用
	6.3 採用單一的日誌紀錄機制，確保輸出格式的一致性		V	V	通用
	6.4 對日誌紀錄進行適當保護及備份，避免未經授權存取			V	通用
會談(Session)管理	7.1 使用者的會談階段，設定該帳號在合理的時間(至多 30 分鐘)內未活動即自動失效	V	V	V	通用
	7.2 使用者的會談階段在登出後失效	V	V	V	通用
	7.3 會談識別碼(Session ID)或使用者 ID 避免顯示於使用者可以改寫處(例如網址列)		V	V	通用
	7.4 會談識別碼(Session ID)採亂數隨機產生且不可預測			V	通用
	7.5 使用者登入後，重新賦予會談識別碼(Session ID)			V	通用
錯誤及例外處理	8.1 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	V	V	V	通用
	8.2 所有功能皆進行錯誤及例外處理，並確保將資源正確釋放		V	V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
	8.3 具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)			V	通用
組態管理	9.1 管理者介面限制存取來源或不允許遠端存取	V	V	V	通用
	9.2 作業平台定期更新並關閉不必要服務及埠口(Port)		V	V	通用
	9.3 系統依賴的外部元件或軟體，不使用預設密碼		V	V	通用
	9.4 參數設定或系統設定存放處，限制存取或進行適當保護			V	通用
	9.5 針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新			V	通用

附件4 STIX 情資格式架構