資通訊產品資安事件企業應變機制手冊

中華民國115年1月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	114/12/26	新編
2	V2.0	115/1/30	1. 配合企業所提意見，調整文件部分內容，以使規範更符合實務運作需求。 2. 經文件內容定稿並轉為正式版本後，調整為正式發布之名稱。
3			
備註			

資料來源：TWCERT/CC 整理

目　次

圖 目 次

表 目 次

1. 前言

隨著產品漏洞揭露日趨頻繁、供應鏈風險逐漸升高，以及第三方通報機制愈加成熟，如何建立具備應變效率與制度化作業流程的產品安全事件應變小組(Product Security Incident Response Team，簡稱 PSIRT)，已成為提升企業資安治理成熟度與強化外部信任的重要步驟。

同時，產品安全也日益受到國際法規與標準的重視，如歐盟「網路韌性法案(CRA)」、「產品責任指令」，以及美國 NIST 等資安機構針對產品安全事件應對的實務框架，皆顯示企業不僅需自主管理產品風險，亦須具備符合監管要求的應變能力。

本手冊旨在提供 PSIRT 建置的實務建議，基於 FIRST 所提出 PSIRT 服務框架為基礎，從組織結構、利害關係人、漏洞處理流程及培訓等層面，系統性地規劃並執行 PSIRT 相關作業，強化產品在整個生命週期的安全事件應對能力。內容以可落地為原則，聚焦於實際推動所需的結構與作法，供組織內相關人員參考使用。

1.1 目的

隨著軟體驅動的產品比例日益增加，產品漏洞不再僅限於硬體設計缺陷，更常見於應用程式錯誤、開源軟體風險、API 曝露或更新機制的安全問題。此外，雲端連線、OTA(Over-The-Air)更新與資料交換也讓產品在整個生命週期內皆暴露於外部威脅之中。

為使企業統一產品安全事件的處理流程，強化跨部門協作，可透過 PSIRT 提升事件應對效率與溝通品質，同時符合國際法規要求，建立對外信任機制，進一步促進產品安全治理能力的成熟與落實。

- 統一處理機制

整合產品開發、資訊安全、維運與法務等部門，建立針對產品相關安全

事件的標準應變流程，無論是韌體漏洞還是軟體更新缺陷，皆能有一致、透明的處理方式。

●提升事件應對與溝通品質

在事件通報、分析、修補與對外溝通，透過明確的角色分工與時效規範，確保資訊流暢傳遞，避免進度停滯。

●符合法規與產業趨勢

面對歐盟「網路韌性法案(CRA)」、美國政府針對軟體供應鏈的強化要求、ISO 30111 與 FIRST PSIRT 標準等國際法規與準則，企業需具備系統化且可追蹤的產品安全管理能力。而現今建立 PSIRT 已非單純的資安最佳實務，而是進入歐盟(CRA)、美國(FCC Cyber Trust Mark)等國際市場的必要合規門檻。缺乏此機制可能導致產品面臨禁售風險或鉅額罰款，直接衝擊企業營收與永續經營

●維護企業信譽與信任關係

當客戶或研究人員通報產品漏洞時，能夠迅速且依循既定流程進行回應與處理，進一步提升企業信任度與品牌形象。

●強化產品安全治理能力

PSIRT 不僅負責處理產品安全問題，亦能將漏洞應變經驗回饋至研發流程，逐步提升產品設計與開發階段的安全成熟度。

整體而言，PSIRT 的設立不僅是回應單一事件的工具，更是企業在軟硬體產品安全治理上的重要戰略資產。

1.2 適用對象

本手冊適用於有意建置或精進 PSIRT(Product Security Incident Response Team)機制的企業或組織，尤其是擁有自主產品開發、數位服務營運、或

對資安合規具有責任的企業組織。面對日益嚴峻的資安威脅與國際法規要求，建立一套制度化且可執行的產品與服務安全事件應變機制，已成為企業資安治理的重要一環。

本指引適用於需負責產品與數位服務安全事件應變工作的企業與組織，特別是具備自主開發、維運產品或服務的平台型、製造型與科技型企業。隨著歐盟《網路韌性法案(CRA)》、NIS2 指令、美國軟體供應鏈安全倡議等國際法規對產品資安要求日益提高，各產業需建立完善的 PSIRT 機制，以有效因應產品與服務在市場上的漏洞風險與外部通報需求。

本指引內容聚焦於組織如何導入與運作 PSIRT 機制，適用對象包括但不限於下列角色與單位：

- 資通訊與軟體產業

  包含提供 SaaS、PaaS、雲端服務或資訊軟體服務的企業。這類企業產品生命週期短、更新頻繁，易受外部通報與零時差攻擊挑戰，急需建立快速回應與透明溝通的事件處理機制。

- 智慧製造與工控設備產業

  例如提供機械、車用電子、醫療設備或 OT 系統的廠商。其產品多含韌體與嵌入式系統，若未妥善管理漏洞風險，將影響關鍵基礎設施與使用者安全。

- 電子與硬體產品製造業

  如半導體、網通設備、IoT 產品製造商，產品具長生命周期與複雜供應鏈結構，需建立通報處理、韌體更新與溝通協調的完整機制，以符合 CRA 等新興法規要求。

- 金融與科技服務業(Fintech)

涉及大量敏感資料與交易系統，常以 API 或 SDK 提供服務組件，也應具備針對第三方組件與自家產品的事件應變能力。

●零售與數位平台服務業

包含提供電商、串流、物流與生活應用平台的企業，當產品與服務為使用者日常所倚賴時，漏洞或資安事件將對信任造成直接衝擊，須快速應對並穩定溝通。

2. PSIRT 模型

本手冊以國際資安組織 FIRST(Forum of Incident Response and Security Teams)所提出之 PSIRT 服務框架(PSIRT Services Framework)為基礎[1]，作為建立產品資安事件應變小組(Product Security Incident Response Team，PSIRT)之參考模型。

由於各組織在營運規模、產業性質、產品類型、組織架構和產品開發策略等方面皆有所差異，因此，並不存在一種可適用於所有組織的單一 PSIRT 建置方式或事件回應流程範例。但是大多數組織採用三種 PSIRT 模型，分別為分散式模型、集中式模型及混合式模型。

2.1 分散式模型(Distributed Model)

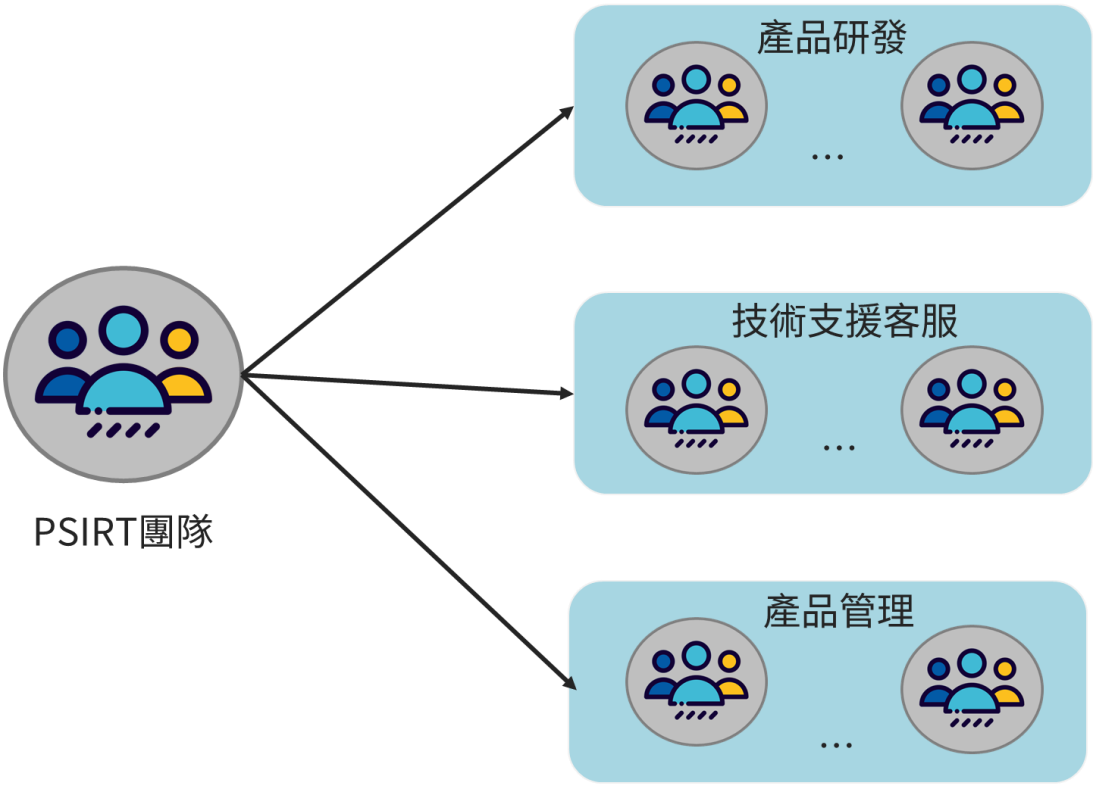
圖 1 為分散式模型的運作方式，是以一個小型的核心 PSIRT 團隊，與組織內分散於各產品團隊中的安全代表進行協作，處理產品的安全漏洞。核心 PSIRT 的主要職責包括制定分類、分析、補救與溝通等相關政策與作業程序，並作為安全漏洞回報的集中接收點，負責分派案件、協助制定修補計畫，並協調通報草稿與事件管理作業。

此模型特別適用於擁有多樣化產品組合或跨部門開發架構的大型企業，能有效發揮現有技術人員的專業能力，同時分攤 PSIRT 的人力與管理成本。在此架構下，組織可建立分層的產品安全制度，由產品研發團隊執行修補與測試工作，核心 PSIRT 則提供整體風險研判與治理建議。

分散式模型具備高度彈性，能快速對應特定產品的安全問題，也便於掌握技術細節與開發脈絡。然而，此模型亦存在制度整合與流程一致性不足的風險，若缺乏中央政策指引與監督機制，容易造成資安作業品質落差，甚至影響對外通報與揭露的準確性與時效性。

因此，採用分散式模型之組織，仍須建立橫向協調與稽核機制，並定期檢

視各單位 PSIRT 作業成效與成熟度，以維持整體資安治理的一致性與透明。



資料來源：FIRST Services Framework

圖1　PSIRT 之分散式模型

總體而言，分散式模型適合資源分布廣泛、產品類型繁多的企業導入，並透過核心 PSIRT 協調整體風險治理，強化組織的漏洞應變能力與跨部門合作效率。

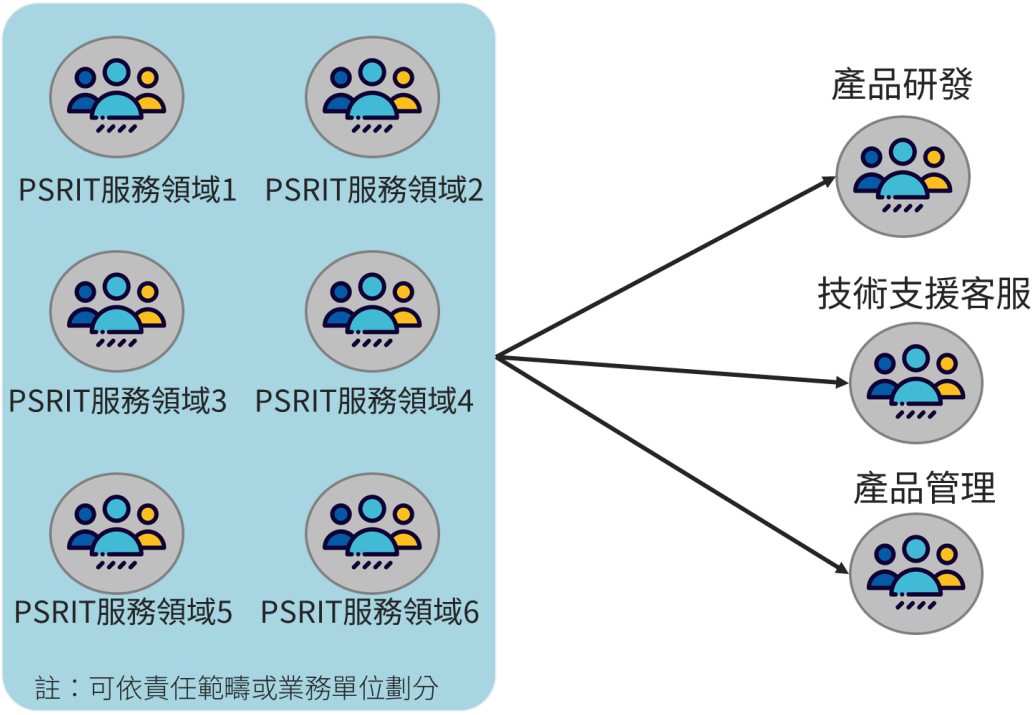
2.2 集中式模型(Centralized Model)

圖 2 為集中式模型係指由一支專責的核心團隊集中處理產品安全事件的各項任務，包括通報接收、漏洞分析、風險評估、修補協調、資訊公告與通報者回應等作業。所有決策權與執行權均集中於此團隊，確保作業流程一致、資訊傳遞明確、應變機制統一。

此模型特別適用於組織規模較小、產品線較為單一或同質性高的企業，能有效整合資源、減少協調成本，並建立高度專業化的事件回應能力。集中型 PSIRT 通常由組織內不同的責任範疇或業務單位共同組成，例如依產品線(如網路設備、雲端服務)、技術領域(如軟體、硬體)或市場區隔(如歐洲、亞太)進行劃分，透過集中配置，組織得以將有限資源投入於建立高品質的資安專業能力，在團隊內部培養一致的流程規範、技術知識與事件處理標準，提升整體回應效率與品質。

此外，集中式模型也利於推動內部制度化流程，例如標準作業程序(SOP)制定、漏洞揭露政策一致性與通報紀錄保存，對於需要法規遵循、供應鏈資安審查或具備稽核需求的組織而言，為一實務上可行且具治理優勢的選擇。

然而，當產品組合多樣或組織規模擴大時，集中式模型可能因無法深入掌握各產品細節與開發流程而導致應變效能下降，需特別強化與產品單位之橫向溝通機制。因此，採集中式模型的組織，應評估其在規模成長後的可擴展性，並考慮導入標準化流程、工具平台與知識分享機制，以維持長期營運穩定性與服務品質。



資料來源：FIRST Services Framework

圖2　PSIRT 之集中式模型

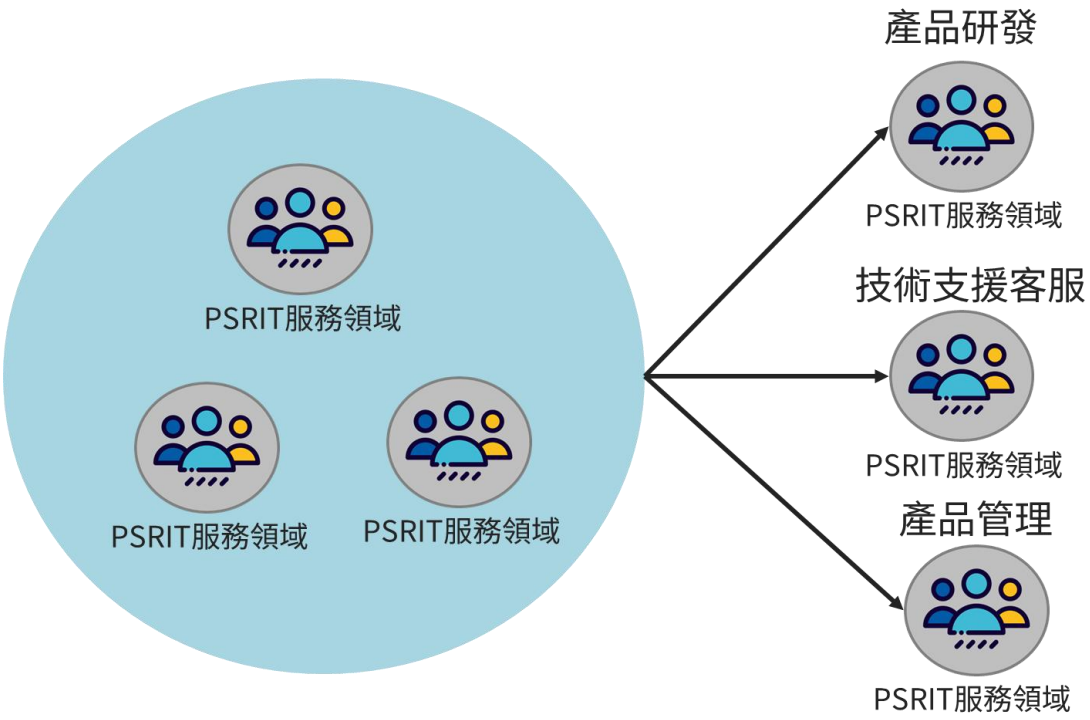
2.3 混合式模型(Hybrid Model)

圖 3 為混合式模型是目前最為常見的 PSIRT 組織模式，兼具集中式與分散式模型的優點。此模型下，組織會設立一個中央 PSIRT 核心單位，負責制訂制度、維護流程標準、統籌通報機制與資訊揭露；同時，各產品或業務單位則配有聯絡窗口或專責人員，負責實際的漏洞評估、修補與測試作業。

混合式模型可靈活對應組織內不同產品線的需求，並確保整體政策的一致性與透明度。此架構特別適用於具中大型規模、產品線多樣且技術架構複雜的組織，特別是產品生命週期管理與供應鏈風險控管需求較高者。例如同時擁有雲端服務、硬體設備與軟體產品的企業。

混合式模型可有效結合集中團隊的制度化管理與各產品部門對自身產品的深厚理解，提升事件應變的效率與品質。因此，採用混合式模型的組織，

應建立清晰的角色分工架構，定期舉辦跨部門協調會議與教育訓練，並透過通報系統、紀錄平臺與稽核流程強化治理，確保制度落實與應變效能。



資料來源：FIRST Services Framework

圖3　PSIRT 之混合式模型

實務導入 PSIRT 時，組織除理解不同 PSIRT 模型的基本概念外，更需依據自身規模、產品組合特性、組織治理結構及資源配置情形，評估組織適用性與可行性。不同模型在運作方式、權責集中程度及跨部門協作模式上各有差異，亦各自具備相對應的優勢與營運挑戰。為協助組織於建置或調整 PSIRT 架構時進行決策評估，以下彙整分散式、集中式與混合式 PSIRT 模型之適用情境、辦理方式、優點與缺點，做為實務導入與組織選型之參考，詳見。

表1　PSIRT 模型比較表

類型	分散式模型	集中式模型	混合式模型
適用情境	適用於產品線多元、組織規模較大，且各產品單位具備一定資安技術能力之企業，由核心 PSIRT 與各產品團隊共同分擔漏洞處理責任。	適用於組織規模較小或產品組合相對同質之企業，集中建立具高度專業能力的 PSIRT 團隊，以統一管理所有產品之漏洞回應作業。	適用於組織規模成長中或產品多樣性逐步擴大的企業，需在集中治理與分散執行之間取得平衡，以兼顧效率與彈性。
辦理方式	設立小型核心 PSIRT 做為統籌與協調角色，負責政策制定、通報集中與對外溝通，各產品或技術單位依分工負責漏洞分析與修補作業。	由單一 PSIRT 團隊全面負責漏洞接收、分析、修補協調及資訊揭露，集中制定決策、流程與資源配置，並對各產品單位提供支援與指導。	由核心 PSIRT 負責整體政策、流程及重大事件決策，各產品單位或區域團隊依授權範圍執行漏洞分析與修補，並透過明確協作機制進行回報與協調。
優點	▪ 適合產品組合龐大且多元的組織。 ▪ 成本可由整個組織分攤。 ▪ 各功能部門可發揮其專業職能。 ▪ 能隨著產品組合成長而具備良好擴展性。	▪ 適合產品類型較為單一或同性質高的組織。 ▪ 預算、政策及資源決策集中管理。 ▪ 對營運具有較高的控制力與明確的分工。	混合式模型結合集中式模型與分散式的特性，部分功能集中管理，其餘則由產品或業務單位分工執行，以平衡治理與彈性

類型	分散式模型	集中式模型	混合式模型
缺點	▪政策與決策僅具部分影響力。 ▪通常無法直接管控實際負責修補漏洞的資源。 ▪各產品團隊可能優先考量自身利益，而非組織整體目標。	▪當產品組合快速擴大時，擴展性有限。 ▪多樣產品情境下，需大量跨部門協作與管理調整。 ▪維持具高度專業能力的集中團隊，故成本較高。	

資料來源：FIRST Services Framework

3. 建置實務

本手冊將以建立 PSIRT 之建置作業為模型，逐步說明建置 PSIRT 之參考步驟，以 Plan-Do-Check-Act(PDCA)循環架構，說明各階段建議執行作業項目，詳見圖 4。建置初期可聚焦於「規劃」與「執行」階段，作為初步建置目標；後續則透過「查核」與「改善」階段的相關作業，持續強化與完善 PSIRT 的運作機制。

●規劃階段(Plan)

PSIRT 建置初期，應先行規劃組織內部之團隊架構與角色分工，確認服務項目、涵蓋範圍及利害關係人，並據此制定作業流程、通報流程及應變原則，以奠定制度基礎。

●執行階段(Do)

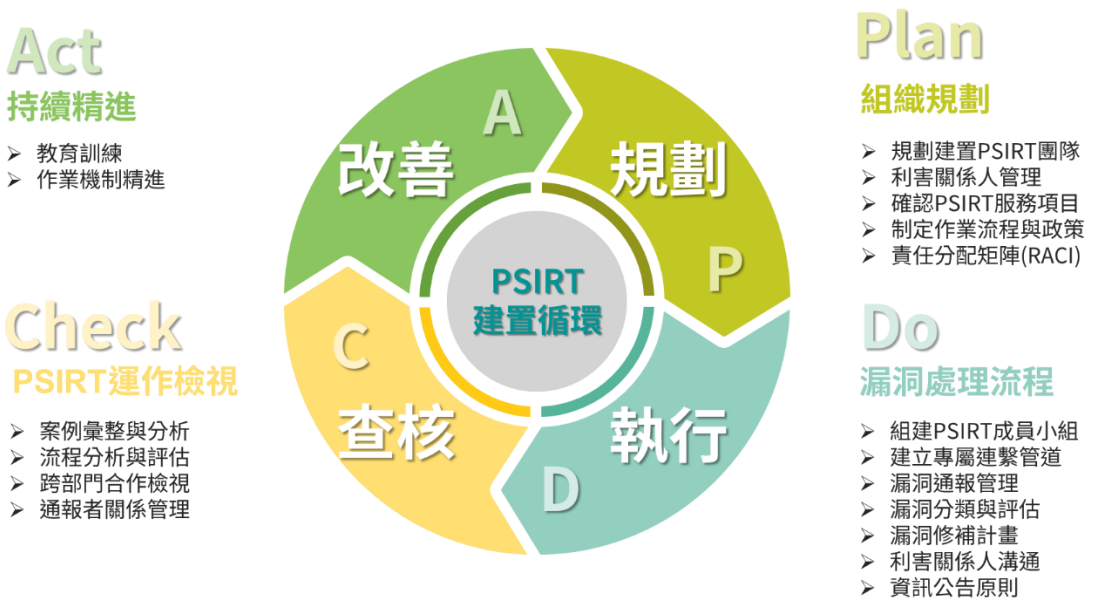
建置 PSIRT 團隊後，PSIRT 應依據既定政策流程，執行日常漏洞管理作業，包含漏洞接收、技術分析、風險分類、修補規劃、通報溝通與漏洞揭露作業，確保事件回應有效落實。

●查核階段(Check)

為確認 PSIRT 運作效能，應定期彙整通報案例、檢視流程執行是否符合法規與內部 SOP，並分析跨部門協作與通報者互動紀錄，以全面掌握制度落實狀況與潛在風險。

●改善階段(Act)

PSIRT 應依查核結果與營運回饋，持續精進作業機制與組織應變能力。透過培訓規劃、演練測試、制度修正及績效指標建立，提升團隊成熟度並強化整體資訊安全治理。



資料來源：TWCERT/CC 整理

圖4　PDCA 建置循環

3.1 規劃階段(Plan)

在 PSIRT 建置初期，首要任務是建立整體規劃架構，釐清組織對 PSIRT 的角色定位與運作期望。此階段須明確界定團隊的職責範疇、服務內容與管理原則，並作為後續制度設計與資源配置的依據。規劃過程中，應全盤考量團隊組成、利害關係人互動、服務內容設定、作業流程設計與責任分工等關鍵要素，使 PSIRT 的職能與目標與組織整體資安策略相互對齊。在這個階段分成五個主要構成要素，包含「規劃 PSIRT 團隊」、「利害關係人管理」、「界定服務範疇」、「制度與流程建置」及「責任分配矩陣」，以下將就前述五設計面向(詳見圖 5)之目的、範疇與實施要點逐一說明。

資料來源：TWCERT/CC 整理

圖5　PSIRT 規劃階段

3.1.1 規劃 PSIRT 團隊

建立具備專業能力與橫向協調能力之 PSIRT 團隊，是建置資安產品事件應變體系的基礎步驟。組織應釐清 PSIRT 的職責定位與角色，並依據產品特性、企業規模及事件應對需求，審慎規劃團隊之成員結構與運作模式，藉此強化事件處置的效率與整體應變穩定性。

PSIRT 小組應至少配置一名具備資安專業能力之產品安全事件協調人員，並視組織規模與產品複雜度，指派負責漏洞分析、通報應對、內部協調與外部溝通等關鍵之成員。同時，應與研發、測試、維運、法務與行銷等關鍵支援單位建立橫向聯繫窗口，落實跨部門支援與資源整合，確保事件處置具備時效性與完整性。

為提升團隊運作效率與一致性，建議同步制定 PSIRT 成員職責手冊或內部作業準則，明確說明各角色日常任務、事件應變分工及通報流程，並可透過定期教育訓練或模擬演練，強化團隊對實務情境之應對能力，進一步提升組織整體資安事件處理能量。

一般而言，PSIRT 團隊的成員通常由專職與兼任人員組成，建議涵蓋以下核心角色與支援角色：

- PSIRT 負責人：負責整體團隊策略方向、內外部協調、資源整合與溝通，確保團隊運作符合法規與內部政策。
- PSIRT 協調團隊：於事件發生期間統籌進度安排、資源調度與通報流程，確保處理時效與一致性。
- 漏洞處理分析團隊：執行漏洞之技術分析與重現驗證，進行風險等級評估，且追蹤修補時程。團隊亦需協助漏洞修補單位制定與驗證修補方案，以確保解決措施之有效性，並避免引入其他潛在風險。此外，負責向相關單位申請 CVE 編號，完成漏洞登記與追溯流程。
- 產品開發團隊：與漏洞處理分析團隊協調修補優先順序與技術風險評估，並協同促進產品安全設計落實。
- 法務與法規顧問：針對相關法規、責任歸屬與對外聲明提供審查意見，確保合法合規。
- 公關部門：協調對外公告文稿與媒體回應，維護組織品牌形象與資訊一致性。
- 客服支援團隊：負責彙整回應用戶之常見問題(FAQ)，處理客戶查詢與疑問。

關於 PSIRT 團隊建置模型之詳細說明，請參閱本手冊第二章。

3.1.2 利害關係人管理

PSIRT 的有效運作倚賴與利害關係人之間良好的協調與溝通機制，也扮演關鍵角色。利害關係人可分為「內部利害關係人」與「外部利害關係人」，雙方在漏洞處理、資訊傳遞、責任分工與信任維護中發揮關鍵作

用。PSIRT 應在建立初期，明確利害關係人範圍，建立持續且制度化的合作關係。

●內部利害關係人

內部利害關係人為企業內部與產品資安事件處理密切關聯的單位，其參與人員可能來自產品開發、產品測試、企業維運、法務、產品行銷、公關等多個相關部門。除了正式編制 PSIRT 成員外，事件處理的有效性亦仰賴橫向跨部門合作機制。以下為雖非 PSIRT 正式成員，卻在資安事件應變過程中扮演關鍵支援角色之內部部門，應於平時建立聯繫機制與作業默契，共同提升處置的準確性與時效性，以利事件發生時快速動員與協作。

– 開發團隊

此團隊為漏洞修補與版本發布之核心執行單位，負責產品程式碼修正、整合與測試，該團隊須與 PSIRT 密切協作，共同執行漏洞之技術評估、風險分析與修補實作。此外，亦可依據事件處理經驗，回饋於產品安全設計中，以持續強化產品之整體資安防護能力。

– 測試與品質管理團隊

該團隊則承擔漏洞重現、修補驗證與回歸測試等任務，協助確認修補後的產品維持功能穩定與安全性，並導入安全測試程序融入日常 QA 作業流程中。

– IT 維運團隊

IT 維運團隊在部署修補版本與服務穩定維護上扮演重要角色。其負責版本更新的實際部署、例行異常監控與突發事件的緊急應變，建議與 PSIRT 建立快速通報管道，必要時納入 CSIRT 流程共同支援應變任務。

– 產品管理與業務單位

產品管理與業務單位負責與評估漏洞影響範圍與商業的整體影響，並協助釐清漏洞公告的優先次序與使用者溝通策略，是資安事件決策過程中不可或缺的橋樑。

– 客服與客戶支援團隊

作為面對客戶的第一線窗口，則需在事件期間回應使用者詢問、提供指引與標準說法，以穩定用戶使用信心。該團隊應配合 PSIRT 提供回應 FAQ、標準範本，並接受必要的流程訓練，以確保資訊傳遞的一致性與準確性。

– 法務與公關部門

對外發布訊息與合規風險評估方面，法務與公關部門協助審查資安公告、通報內容及可能涉及的法律責任，確保組織回應符合法規、品牌定位與外部監管要求。

– 高階管理層

高階管理層在 PSIRT 運作中扮演決策與資源支持的關鍵角色，其負責政策方向指導、資源調配與事件等級判斷，並視事件嚴重性提供對外說明與組織回應支援。PSIRT 應定期向高階主管報告營運績效、潛在風險與重大事件處理狀況，以爭取持續關注與長期支持，確保資安治理於組織內部獲得制度化與策略性落實。

●外部利害關係人

PSIRT 在處理產品安全事件時，不僅與企業內部部門協調合作，亦須面對多元的外部利害關係人。而這些外部單位對 PSIRT 的信任度、回應品質與合作流程，直接影響企業在事件處理的公信力與用戶信賴。因此，

有效管理外部利害關係人，是提升事件處置品質與透明度的關鍵要素。

– 使用者與顧客

使用者與顧客是最直接受漏洞影響的群體，依賴 PSIRT 及時提供、清楚且具有可行性的公告與修補資訊。因此，建立穩定的對外公告渠道、定期發布安全建議，是 PSIRT 對終端用戶的基本責任。此外，對具有高風險資安產品，應考慮建立多語系常見問答(FQA)資源，以強化使用者溝通的透明度。

– 供應鏈與第三方廠商

供應鏈中的第三方廠商、元件供應商或外包開發團隊，亦屬於關鍵利害關係人之一。PSIRT 在發現涉及第三方元件的漏洞時，應主動與廠商聯繫協調修補與公告時程，確保資訊與回應一致性。為強化應變效率，亦主動與合作廠商建立聯絡窗口、簽訂資安義務條款，並定期檢視彼此的通報流程與修補時效。

– 外部通報者

資安人員、白帽駭客或開源社群等，是 PSIRT 發現產品弱點的重要協力對象，為建立信任互動與降低公開風險，建議明確定義漏洞回報政策並適度表彰貢獻者，鼓勵持續合作，亦可考慮導入漏洞獎勵制度或提供回報證明，建立正向互動文化。

– 產業聯盟與資安訊息分享組織

– 產業聯盟、CERT(Computer Emergency Response Team)、ISAC(Information Sharing and Analysis Center)等資訊共享組織，也是 PSIRT 在漏洞協調與事件分析時的重要組織。透過參與這些資安組織，PSIRT 能夠取得威脅情資、漏洞指標、CVE 編號協調支援等資源，有助於提升整體事件處置的標準化與資訊。

另外，PSIRT 可與 TWCERT/CC 漏洞聯繫小組建立正式聯絡窗口，於發現重大產品漏洞、影響廣泛用戶、或涉及跨廠商情境時，善用其協調資源、協助進行通報、轉知及資訊同步處理。

– 主管機關與法規單位

部分產業(如醫療、金融、關鍵基礎設施等)須遵循特定資安法規與主管機關規範，PSIRT 在發現涉及此類產品的漏洞時，應與法務或合規部門合作釐清通報義務，包括通報內容、回應時限與格式要求外，亦主動評估漏洞潛在影響範圍，並與內部相關單位協調，適時提醒產品使用機關單位，建議其儘速採取修補行動。

若產品漏洞已導致企業用戶發生實際資安事件，如資料外洩、服務中斷等，PSIRT 應協助企業用戶依據適用法規啟動事件通報程序。如台灣證券交易所發布「上市公司重大訊息發布應注意事項參考問答集」，明確規範上市公司發生資安事件造成重大損害或影響，即應發布重大訊息。

特別是組織產品屬於政府採購、關鍵基礎服務或已廣泛部署情境下，PSIRT 可透過官方信函、技術通報或配合客戶關係管理機制，協助推廣修補資訊，降低弱點擴散風險。

3.1.3 界定服務範疇

規劃 PSIRT 運作架構時，明確界定其服務項目與職責範圍是確保團隊功能有效落實的基礎。PSIRT 的任務雖圍繞在產品資安事件的處理上，但實際涵蓋的服務項目可能隨組織的產品型態、資安成熟度及對外承諾而有所不同。故在建置階段，應盤點可行的服務範疇，並與相關單位協調確認最終定位，作為後續資源投入、流程設計與溝通準則的依據。一般而言，PSIRT 的核心服務項目包括產品漏洞通報的接收與評估、技術研判與風險

分級、跨部門協調漏洞修補作業、對外公告以及主管機關或產業聯盟的通報協作等。此外，視組織需求同，PSIRT 亦可能負擔起事後分析與經驗回饋、資安事件報告撰寫、安全開發建議、客戶支援技術等延伸職能。

PSIRT 的角色並非單一部門可完全承攬，其運作亦依賴內部利害關係人的協同合作，尤其是面對需要公開揭露或符合法規通報義務的情況下，PSIRT 應針對內部與外部利害關係人建立清楚的服務範圍界線與溝通窗口，包含明確說明受影響的產品範圍、回應時效標準、資訊揭露政策(如 CVE 編號申請政策)、以及使用者端修補建議的提供方式等。

此外，PSIRT 的服務項目應在初期建置階段即進行確認與文件化，並定時檢視其適用性與完整性。唯有明確定義服務內容，才能在有限資源的情況下聚焦於關鍵職能，並確保在資安事件發生時，有章可循、高效協作。

3.1.4 制度與流程建置

PSIRT 團隊的有效運作，必須制定一套標準化、可執行且可追溯的作業流程與政策機制之上。這些機制不僅協助團隊於資安事件發生時能迅速啟動應變，亦能確保溝通準則一致、作業符合規定要求，並可作為組織內外部利害關係人溝通與協作的共同基礎。以下是建議需要制定的作業流程與政策機制。

- 產品漏洞處理流程

制定產品漏洞處理流程是 PSIRT 最基本且核心的政策之一，為建立系統化且可重複執行的產品漏洞處理流程，PSIRT 可依事件處理生命週期，規劃自通報接收至後續回饋的完整作業階段。該流程應涵蓋漏洞接收與初步處理、漏洞技術分析、修補方案制定與實作、資訊揭露與公告發布以及後續追蹤與經驗回饋，詳見圖 6。

每個階段應明確定義職責分工、處理時限、交付成果與審核節點，並根

據漏洞的研究程度設計對應的應處策略與回應時程，以確保事件處理具效率與一致性。為提升流程可行性，建議同步建立對應的作業指引文件(SOP)、通用範本(如漏洞揭露公告格式、回應信件)與記錄表單，作為PSIRT 及各相關部門啟動作業的依據，強化整體執行力與跨部門協作效率。

資料來源：TWCERT/CC 整理

圖6　產品漏洞處理流程

– 漏洞接收與初步處理

建立多元通報管道，接收來自內部部門、外部研究人員、第三方協力廠商等產品漏洞通報。PSIRT 負責進行初步檢視與有效性篩選，並據以進行事件編號、分類及通報回覆等作業。

– 漏洞技術分析

技術團隊針對漏洞成因判斷、影響範圍界定與可利用性驗證，並依據CVSS(Common Vulnerability Scoring System)進行風險評估，以作為漏洞修補優先順序與對外通報策略之依據。

– 修補方案制定與實作

PSIRT 應協同開發或工程團隊提出修補建議，完全修補程式之開發、整合與測試作業，並進行內部品質驗證與版本發布，確保修補措施的有效性與穩定性。

– 資訊揭露與公告發布

依據組織既有之產品資安資訊揭露政策，於適當時機透過網站公告、CVE 公開、電子郵件或其他通報管道，向受影響之利害關係人揭露漏洞資訊，並同步提供修補建議與操作指引。

– 後續追蹤與經驗回饋

PSIRT 應持續追蹤使用者修補落實情形與成效，必要時提供技術協助。事件結束後，應彙整處理過程與改善建議，納入事件回顧報告，作為日後流程精進與訓練教材之依據。

– 非正常漏洞處理流程

在實務運作中，部分漏洞可能無法完全符合預先設計的標準流程，例如未經授權即公開揭露資訊，或供應鏈元件揭露造成間接影響等。應對此類「非正常」事件流程，PSIRT 應建立具備彈性的處理機制，確保在資訊有限、情勢緊急或決策不明確的狀況下，仍能快速評估風險、整合內部資源並進行有效應變。

– 產品漏洞通報政策

促進資訊安社群協作、提升組織產品安全性與事件回應效能，應建立正式的產品漏洞通政策，提供給研究人員、用戶、廠商合作夥伴與第三方通報的正式管理與處理流程。該政策同時應銜接國際資安漏洞揭露體系與國內通報協調單位，強化資訊透明度與跨組織協作能力。

➢申請 CVE 漏洞編號

若組織已向 MITRE 申請並取得 CVE 編號管理者(CVE Numbering Authority，CAN)資格，則具備對所屬產品之漏洞通報、核發 CVE 編號與撰寫公開描述的責任。

如組織尚未取得 CNA 資格時，可由 TWCERT/CC 協助組織申請 CVE 編號。此途徑雖需依賴第三方進行處理，但仍可確保漏洞獲得正式登錄與國際認可，並有助於建立組織對於資安事件應對的制度化流程。

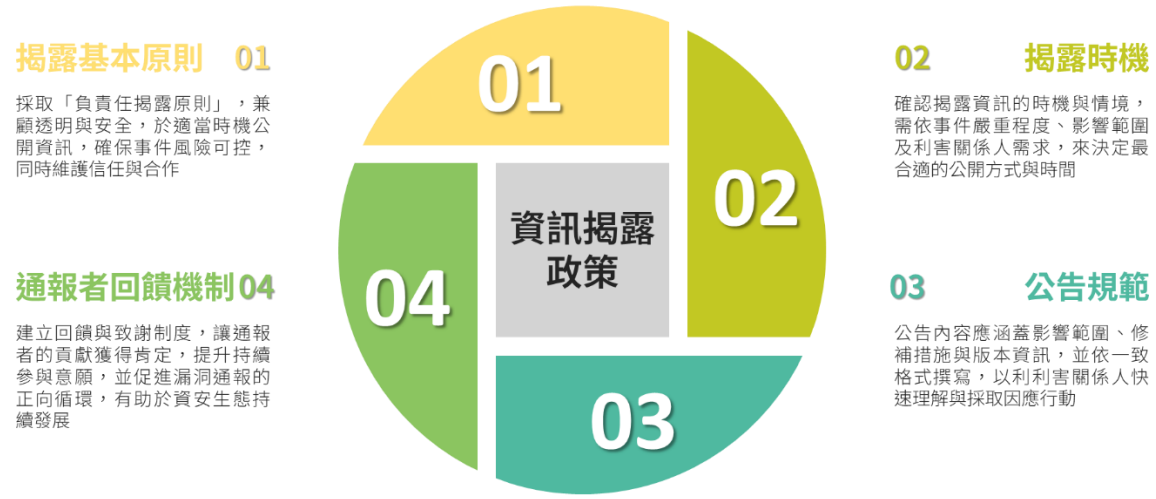
➢與 TWCERT/CC 合作機制

為進一步強化漏洞處理的透明度與信賴基礎，PSIRT 組織可與 TWCERT/CC 漏洞聯繫小組建立合作機制。當發現產品漏洞時，除內部處置外，亦可依情境通報 TWCERT/CC，由其協助進行 CVE 漏洞編號申請與公告發布作業。若遇通報內容涉及多方利害關係人，TWCERT/CC 亦可作為第三方協調單位，協助追蹤漏洞源頭並促進溝通，避免漏洞持續擴散或處置延誤。

透過此合作機制，PSIRT 不僅可強化漏洞揭露程序的完整性與可信度，亦有助於建立國內資安協調體系的聯繫與互信，促進整體資安通報體系的健全發展。

➢產品資訊揭露政策

為強化組織在產品安全事件處理過程中的資訊透明與利害關係人溝通，PSIRT 應建立明確的產品資訊揭露政策，作為對外說明資安事件與漏洞資訊的準則。此政策核心在於兼顧資訊正確性、風險控管與合規需求的前提下，確保用戶、合作夥伴與主管機關能即時取得必要資訊，降低資安事件對產品使用者與組織聲譽的衝擊。此政策建議涵蓋資訊揭露基本原則、揭露時機與考量情境、公告內容範疇與格式、以及通報者回饋與致謝機制(詳見圖 7)。



資料來源：TWCERT/CC 整理

圖7　產品資訊揭露政策

➢揭露基本原則

PSIRT 以保障使用者安全與降低風險為首要原則，採取「負責任揭露原則(Responsible Disclosure)」，兼顧通報者權益與組織營運考量。揭露時應避免在修補措施尚未完成前公開可能導致濫用之漏洞資訊，確保資訊揭露的安全性與審慎性。

➢揭露時機

原則上應於修補方案可供部署時，同步對外公開漏洞資訊。若遇特殊風險情境(如多方協調修補、尚無解法、易被濫用等)，可採取階段性揭露或延後公開策略。若發生重大緊急事件，PSIRT 可與高階管理層共同研判是否提早公告並發布預警資訊。

➢公告規範

公開資訊內容應完整且明確，至少包含漏洞識別碼(如 CVE 編號)、影響產品與版本範圍、風險描述(含 CVSS 分數)、修補建議與更新方式、聯絡窗口資訊方式。必要時亦可補充攻擊跡象(IoC)、臨時緩解

措施或安全建議，協助利害關係人妥善應對。

➢通報者回饋機制

為鼓勵第三方通報者持續參與，PSIRT 應建立公開致謝與回饋機制，尊重其貢獻並提升合作意願。可視需求提供匿名通報選項、指定聯繫窗口與回報證明，以保障通報人身分與權益，營造正向的協作文化。例如，設立公開名人堂(Hall of Fame)頁面表揚通報者、提供感謝信與電子證書作為其貢獻記錄，並視組織資源狀況導入漏洞獎金制度(Bug Bounty)，強化外部參與動機，建立互信合作的資安生態圈。

3.1.5 責任分配矩陣(RACI)

為了確保 PSIRT 在各階段作業中具備清晰且一致的責任分工，建議導入責任分配矩陣(Responsibility Assignment Matrix，簡稱 RACI)。RACI 模型有助於明確界定各項任務中相關人員的角色與責任，避免重工、遺漏或權責不清的情況，提升跨部門協作效率與決策透明度，詳見圖 8。

資料來源：TWCERT/CC 整理

圖8　RACI 模型

RACI 模型中四項角色分別為：

●R(Responsible)執行者

指實際負責執行某項任務的個人或團隊，需確保任務按計畫完成。每項

任務至少指定一位負責者，亦可有多人協同參與。

●A(Accountable)當責者/(Approver)核可者

對任務結果負最終責任者，通常具決策權或任務核可權，需確認任務已妥善完成。為避免責任混淆，每項任務應僅指定一位當責者。執行者所提交的成果，須經由當責者審核與確認才正式生效。

●C(Consulted)受諮詢的專業者

於執行任務前或過程中提供專業建議的相關人員，通常具備特定技術領域知識或掌握關鍵資訊，與執行者進行雙向溝通。此角色有助於提高決策的正確性與執行的全面性。

●I(Informed)需被告知的人員

雖不直接參與任務執行，但需掌握進度與結果以因應其業務職責。通常透過報告、公告或簡報等方式接收單向資訊，以利風險控管與資源調配。

RACI 模型能作為 PSIRT 漏洞處理任務的標準分工框架，建議組織針對常見情境建立對應的 RACI 表格，並納入 PSIRT 作業手冊，作為溝通、協作與責任落實的制度性依據，以強化團隊應變能力與管理一致性。表 2 為 RACI 基本格式，可根據組織實際規劃自行規劃。

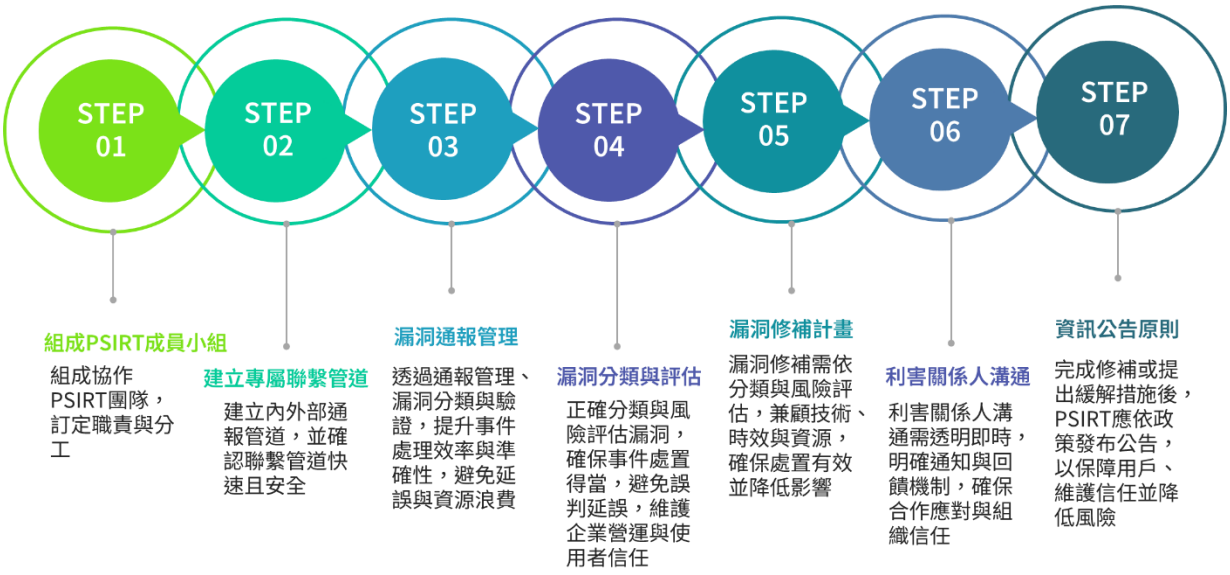
表2　RACI 範例

部門	部門 1	部門 2	部門 3	部門 4	部門 5
任務 1					
任務 2					
任務 3					
R：負責者、A：當責者、C：事先諮詢者、I：事後告知者					

資料來源：TWCERT/CC 整理

3.2 執行階段(Do)

在完成 PSIRT 的規劃架構後，進入執行階段便成為確保制度化設計得以落實的關鍵。本階段聚焦於將前期所制定的政策、流程與角色分工轉化為具體可操作的實務作業，涵蓋團隊組成、通報管道建置、漏洞處理流程的啟動與執行，直至風險通知與資訊揭露等核心環節。PSIRT 應依據規劃階段所建立之政策基礎與責任機制，正式啟動其運作模式，並在真實事件的處理過程中持續檢視與提升應變能力。為協助各組織系統地建構完整的執行能力，本章節將逐一說明執行階段所涵蓋的七項關鍵實務構面，詳見圖 9。



資料來源：TWCERT/CC 整理

圖9　PSIRT 執行階段

3.2.1 組成 PSIRT 成員小組

完成 PSIRT 成員編制與職責規劃後，執行階段的首要任務即為實際成立

PSIRT 成員小組，確保關鍵人員到位，並具備執行產品資安事件處理所需之能力與資源。本階段應依據各組織所擬定之組織結構、成員角色與支援團隊關係，完成實體團隊編組與職責確認作業。

3.2.2 建立專屬聯繫管道

為確保產品漏洞能被及時發現與處理，PSIRT 必須建立完善且明確的漏洞通報與聯繫管道，這些管道應涵蓋內部與外部的通報來源，並確保通報資訊的安全性與完整性。

●外部通報

PSIRT 應對外公開專用的漏洞通報管道，建議在公司官方網域下設置專屬郵件地址，如 psirt@、incidents@、security@等，並提供清楚且易於遵循的通報指引，以利外部研究人員、合作夥伴及使用者能迅速且準確提交漏洞資訊。此外，建議依循 RFC9116 所定義之 security.txt 標準，於官方網站對外公開的網域中設置 security.txt 檔案。該檔案必須以純文字(plain text)格式撰寫，並採用 Net-Unicode 形式之 UTF-8 編碼，且應透過 HTTPS 提供予外部通報者存取；檔案通常放置於 /.well-known/security.txt、網站根目錄或其他慣用公開目錄。此作法已獲美國網路安全暨基礎設施安全局(CISA)倡議，並被視為提升漏洞通報可達性與通報通知效率之重要實務措施。

其內容至少應包含安全漏洞通報之聯絡方式(Contact)及檔案有效期限(Expires)，其餘建議性或選擇性欄位，可參考 CISA 所發布之 security.txt: A Simple File with Big Value (https://www.cisa.gov/news-events/news/securitytxt-simple-file-big-value)或 RFC 9116：A File Format to Aid in Security Vulnerability Disclosure (https://www.rfc-editor.org/)，以作為內容設計與實務導入之依據。

另外，保障資料之機密性及防範資料遭竄改，亦建議通報管道支援 PGP(Pretty Good Privacy)或其他安全加密機制，提供通報者加密其敏感資訊的能力。具體加密方式可採用受 S/MIME 或 PGP 保護的電子郵件，或採用啟用 HTTPS 的安全 Web 表單，確保通報過程安全可靠。

●內部通報

在內部通報部分，除了建立專屬的內部漏洞通報流程與渠道外，建議組織鼓勵內部人員使用與外部通報相同的管道，例如專用的安全通報電子郵件地址，讓內外部通報方式保持一致，降低資訊流轉的複雜度。此舉有助於漏洞資訊集中管理與追蹤，方便 PSIRT 統一受理及調度。

若組織需額外建立專屬的內部通報管道，可透過內部系統、專屬郵件群組或即時通訊工具實施，並指定專責窗口負責漏洞資訊的接收與分派，確保內部通報流程的效率與透明度。同時，為保障通報內容的安全性，內部通報亦建議支援 PGP 加密等安全措施，以確保敏感資料之機密性。

●向 TWCERT/CC 通報

若組織本身尚未成為 CNA，在處理產品漏洞時，若需取得 CVE 編號，則可透過 TWCER/CC 作為協助窗口，申請對應的 CVE 編號，確保漏洞資訊能被正式編錄並追蹤，相關說明與作業方式請參閱官方網站 (https://www.twcert.org.tw/tw/np-131-1.html)或詳見附件 2。

綜上所述，漏洞通報不僅是 PSIRT 工作的基礎，也是保障產品安全的第一道防線，應持續精進並保持暢通，以促進快速、有效漏洞發現與應對。

3.2.3 漏洞通報管理

在產品事件處理流程中，首要步驟始於接獲一則通報，或由內部主動發現潛在風險。此階段對漏洞來源管理、通報流程設計，以及對漏洞真實性與嚴重程度的初步判斷，是整體 PSIRT 作業的基礎。若流程不明確或判斷失

誤，將可能導致事件處置延誤、誤報與濫報增加，不僅消耗組織資源，更可能損及企業信譽。

為提升漏洞處理流程效率與正確性，應從以下四個面向著手，分別是漏洞來源與通報管理、漏洞類型與初步歸類、新舊漏洞識別與比對，以及漏洞重現與初步技術驗證。這些步驟雖屬初期作業，卻決定了後續處置流程的準確性與調度優先級，應予以系統化規劃。

●漏洞來源與通報管理

本階段之漏洞來源管理，與 3.2.2 所述之建立專屬漏洞通報與聯繫管道密切相關。組織應充分運用既有的外部與內部通報管道，確保能有效接收來自多元通報者的漏洞資訊，並建立相應的回應與追蹤機制。這些通道不僅用於被動接收通報，亦應結合主動式監控策略，持續關注外部資安訊息來源，例如：資安研究社群、社交媒體、開源專案論壇及威脅情報平台等，從中擷取與本產品潛在相關的漏洞訊息。

此外，PSIRT 團隊應積極拓展通報來源，除被動接收通報外，建議主動與開源社群、學術機構及白帽駭客建立合作關係，不僅有助於提前掌握潛在風險，亦能培養互相基礎，推動正向的漏洞揭露文化。此舉有助於建立良性的通報回應循環，進一步提升整體資安生態系的成熟度與應變能量。

同時，也應注意來自資安聯防體系的通報來源，TWCERT/CC 為台灣資安協調與支援中心，亦能協助通報者與廠商建立聯繫，將相關漏洞資訊轉知供應商進行後續應處。為強化跨單位協作效能，建議 PSIRT 預先與 TWCERT/CC 之聯繫窗口與合作機制，確保能即時獲取必要資訊並妥善應對潛在風險，進一步提升事件應變的完整性與效率。

●漏洞類型與初步歸類

為避免重複處理或誤判情形，PSIRT 應執行漏洞唯一性識別作業，此作業包括比對現有已揭露漏洞資料來源，例如 NVD、MITRE CVE 資料庫，以及組織內部漏洞追蹤系統等，以確認該通報是否屬於全新漏洞，或為既有問題之變異、重現或延伸影響。此步驟亦為判斷是否需申請 CVE 編號的重要依據。

在處理漏洞通報時，PSIRT 應具備辨識漏洞所屬範疇的能力，以利後續技術分析、責任歸屬及修補工作的明確分工。一般而言，產品相關漏洞可依其來源區分為下列三種類型：

1. 產品本身程式碼漏洞：源自組織自行開發之產品原始碼中所產生的安全漏洞，修補與改善工作可內部開發團隊負責修補與版本發布。
2. 供應商內部維護元件漏洞：來自外部供應商自行開發並維護的元件所產生的漏洞。雖非組織自行開發，但可由該供應商提供修補建議與更新。
3. 第三方元件整合漏洞：指產品中所使用的供應商所整合的第三方元件，如開源套件、商用函式庫等所產生的漏洞。此漏洞需透過供應商追溯原始來源，並等待上游單位提供修補措施或資訊。

釐清漏洞的來源不僅有助於 PSIRT 明確識別修補責任與追蹤更新進度，也有助於判斷是否需主動發布安全公告或協助供應商聯繫上游單位進行修補，並針對不同來源漏洞建立應對的回應策略與溝通流程，確保漏洞能夠在最短時間獲得適當處置，是強化產品資安治理與應變效率的基礎。

●新舊漏洞識別與比對

若確認為新漏洞，應即時登錄至內部漏洞處理系統，並依據標準作業流程(SOP)啟動後續處置流程；若判定為既有漏洞之延伸或影響範圍擴大，

則應整合至原始事件編號統一追蹤與管理，以利後續追蹤與風險評估作業的完整性或一致性。

此外，建議組織內部可積極參與新漏洞的揭露，若漏洞係由組織內部主動發現並確定，可大幅降低與外部通報者的溝通協調成本，避免因資訊不對稱導致處理時程延誤或技術細節誤解，亦能掌握揭露時機與內容主導權。若由組織主動揭露漏洞，不僅可展現對產品資安的重視與透明治理的承諾，也助於建立外界信任、提升品牌聲譽。長期而言，這將形成正向循環，讓組織能更有效率處理產品安全議題，並強化其在產業與社群中的資安專業形象。

●漏洞重現與初步技術驗證

完成漏洞唯一性識別與來源分類後，PSIRT 應進行初步技術驗證，以確認漏洞是否重現。此作業通常由具備資安分析能力的人員負責，根據原始通報內容或自行撰寫測試腳本，驗證漏洞存在與否，並記錄其觸發條件、環境依賴與漏洞重現步驟。

若漏洞無法重現，應主動聯絡通報者取得更多技術細節，或經評估後合理結案。重現結果不僅作為漏洞是否進入修補流程的重要依據，也有助於後續修補人員理解漏洞成因與觸發途徑，提升修補工作的效率與準確性。

3.2.4 漏洞分類與評估

在漏洞管理流程中，正確分類漏洞並評估其風險等級，是確保事件能被妥善處置的關鍵環節。此階段的核心目的在於釐清漏洞的技術屬性與影響範圍、判斷應對的急迫性，提供應處決策的依據，並協助相關部門有效規劃修補與溝通作業。若分類與風險評估不精確，將可能導致風險誤判，處置延遲或反應過度，進而對組織營運與使用者信任產生負面影響。

●漏洞技術屬性與來源歸類

為有效支援漏洞應對策略之制定，PSIRT 應接收通報並完成初步驗證後，對漏洞進行多面向的歸類與標記。此步驟不僅有助於後續分析與修補工作的分工與規劃，也能提升整體漏洞管理的可視性與系統性。

在技術層面，應針對漏洞的行為特徵進行分類，常見的分類方式包含：

– 漏洞類型：建議依據 CWE(Common Weakness Enumeration)所提供之弱點分類進行歸類[2]，以利標準化管理與後續統計分析。常見類型包含：緩衝區溢位(Buffer Overflow)、跨站腳本(XSS)、SQL 注入(SQL injection)、權限提升(Privilege Escalation)、身分認證繞過(Authentication Bypasses)等。

– 影響模組：應標示出具體受影響的元件與模組，例如 Web UI、API 服務、韌體模組、驅動程式、資料庫等。

– 影響範圍：包含單一產品功能、整體平台架構、跨產品共用模組，甚至雲端端點或伺服器端等。

在來源層面，則需釐清漏洞的產出背景與責任歸屬，詳細可參考 3.2.3 所述之漏洞類型與初步歸類。

正確識別漏洞的技術屬性與來源，除了有助於修補責任明確化與技術處置分層外，也可建立可供趨勢統計、風險聚焦與未來防範機制設計的數據基礎。建議 PSIRT 於漏洞處理系統中，建置可結構化紀錄上述分類欄位，並定期主動向利害關係人報告。

●風險評估指標與方法

有效判斷漏洞對產品與用戶可能造成之影響，PSIRT 應導入一套或多套風險評估方式，建立一致、可溝通且具決策參考價值的評分與分級機

制。以下是常見之風險評估指標：

– CVSS(Common Vulnerability Scoring System)

CVSS 是目前最廣泛採用的漏洞風險評分標準，由 FIRST 組織所維護[3]，提供一致性高、可量化的評分機制。2023 年 11 月 FIRST 推出 CVSS v4.0，以改善評分準確度與針對現代威脅的表達方式，但目前多數的通報平台仍以 CVSS v3.0 為主要版本。因此，PSIRT 可採取雙版本並行策略，以確保與主流平台相容。

– MITRE ATT&CK Framework

MITRE ATT&CK 為針對已知攻擊技術與行為所建構之分類架構，廣泛應用於資安威脅建模與防禦策略設計[4] 。對 PSIRT 而言，ATT&CK 可做為漏洞風險評估的輔助工具，協助分析特定漏洞在整體攻擊鏈中扮演的角色與影響範疇。

– TLP(Traffic Light Protocol)

TLP 最初由 FIRST 組織推動，目標在於促進跨組織資訊分享的保密等級共識。TLP 1.0 版文件於 2016 年 8 月 31 發布，目的為確認 TLP 的詮釋具一致性，且用戶群體之間有明確預期；TLP 2.0 版文件於 2022 年 8 月發布，進一步調整分類標籤與應用情境。舉例而言，TLP:RED 表示資訊僅限特定人員知悉，不得再轉傳；TLP:AMBER 表示可在組織內部傳閱。此機制有助於在處理機敏通報避免資訊外洩。目前 FIRST 建議使用 TLP 2.0 版本，詳細內容可至 FIRST 官方網站查閱[5]**錯誤! 找不到參照來源。**。

– 組織自訂風險分級機制

除上述通用指標外，組織亦可依實務需要制定更貼合自身風險評估規則，例如依「緊急、高、中、低」四級分類漏洞，並納入額外變數進

行加權判斷。

綜合運用上述指標與方法，PSIRT 可建立具一致性與可解釋性的風險判定流程，協助決策單位明確掌握漏洞嚴重性，並依據風險等級調整處理時效與資源分配優先順序。

●評估結果應用與應變規則

完成漏洞分類與風險等級評估後，PSIRT 應依據評分結果制定明確的應變作業準則，確保漏洞處置具可預測性與操作一致性。透過對應漏洞類型與風險等級自動產生處理建議，可提升決策效率與標準化程度，亦有助於持續強化 PSIRT 的實務執行能力。常見的應變規則可包含以下面向：

– 處置時效規定

依風險等級設定修補期限，可參考國際標準與業界實務建議，如高風險漏洞於 7 日內完成修補與測試，中風險於 30 日內，低風險納入例行更新週期。實際時效應視組織資源與產品調整。

– 利害關係人通知原則

針對影響層面較廣泛或涉及特定客戶之漏洞，應依風險等級決定是否需提前通知相關利害關係人。

– 揭露政策參考

評估結果亦為制定公開揭露時機與範圍的依據，高風險或具公共安全影響之漏洞，應於修補完成後儘速揭露，確保相關利害關係人能即時防範。

●例外情境與應變彈性

在實務執行中，PSIRT 可能遇到部分漏洞無法立即修補、無法重現、風

險極低或修補成本過高時，為避免處置遺漏或主觀判斷誤差，應建立例外處理機制。

當出現上述情形時，PSIRT 應詳實記錄技術分析過程、風險研判一句與暫不修補的理由，並提報資安管理單位或資安長等具審核權責之單位審查通過，方可列為例外處理項目。

此外，相關處理紀錄應妥善保存，作為未來稽核、改進修補策略、更新風險評估模型或調整通報處置準則之依據。透過持續回顧與案例分析，能有效提升組織應對非典型漏洞事件的決策品質與因應能力，強化整體漏洞管理體系的成熟度。

3.2.5 漏洞修補計畫

漏洞修補是 PSIRT 作業流程中最具技術挑戰與資源投入的核心階段，須依據前一階段(3.2.4) 所完成的分類與風險評估結果，擬定合適的處置策略。有效的修補方案不僅需涵蓋技術面執行，更須考量時效性、資源分配、產品生命週期與使用者的影響。

●修補策略規劃

PSIRT 應根據漏洞的技術類型、風險等級、受影響產品與模組，制定修補策略。此階段亦可規劃是否採用短期緩解措施以爭取修補時間，並評估是否需進行客戶溝通或版本同步機制的準備。

●修補責任分工與時程規劃

針對漏洞影響的範疇不同，應指定適當部門負責修補工作。若漏洞屬於自家產品原始碼範疇，則由內部研發團隊負責修補；若涉及第三方元件(如外部套件或合作廠商提供之元件)，則由採購等單位協助向供應商取得更新，並由 PSIRT 協助採購單位於合約中納入「安全需求(Secure by Demand)」條款，要求上游廠商建立 PSIRT 窗口並承諾修補時效

(SLA)。

為確保風險受控，若遇技術瓶頸或特殊業務需求，應設立例外申請流程以留存決策紀錄。此外，若上游供應商無法即時提供修補(如已 EOL 或無回應)，PSIRT 應具備獨立評估風險之能力，主動發布緩解措施或虛擬修補建議，而非被動等待，以落實對終端客戶的安全責任。

●修補實作與技術測試

進行實際修補時，須先確認漏洞可重現並釐清修補目標。修補作業由專責人員負責，並依標準作業程序(SOP)進行版本管理與程式碼修改。修補完成後，須透過技術驗證確認修補成果，避免出現「修補失敗」或「功能異常」之情況。必要時，PSIRT 可協調資安團隊進行額外的滲透測試或模擬攻擊，以確保修補品質符合既定資安標準。

●修補版本釋出與內部紀錄

完成漏洞修補與測試後，應將更新內容納入正式版本或補丁中發佈，並依據產品特性決定公告方式。例如官網公告、電子報、客戶信件或 API 變更通知等形式對外說明，同時揭露 CVE 編號、風險等級、受影響版本與建議更新方式。內部則應建立完整記錄，包括修補時間點、參與人員、修改內容、測試結果與公告紀錄，以利後續追蹤與稽核，並做為未來應變流程改善的重要依據。

3.2.6 利害關係人溝通

在漏洞處理流程中，與利害關係人有效溝通不僅關係資訊透明與信任維繫，更直接影響事件應變的效率與組織聲譽的管理。PSIRT 除了負責完成漏洞的技術分析與修補作業外，亦應主動規劃溝通策略，依據事前制定的利害關係人分類與分級原則，建立明確的通知準則與資訊傳遞機制。

在事件處置的各個階段，應以透明、即時且一致的方式，將正確資訊傳遞

至適當對象，並促進跨部門及外部協力單位的協同應對，以提升整體處置效能與組織可信度。

通知原則應遵循「誰需要知道、何時知道、需要知道什麼」，避免資訊過度擴散或延誤關鍵通報。而在溝通方面，應強調「資訊的雙向性與回饋」機制，不僅限於單向通知。PSIRT 應確保利害關係人能充分理解通報內容，並設立專責聯繫窗口以接收意見或支援需求，進一步促進跨部門協作與即時回應。

●利害關係人辨識與通知

本手冊於 3.1.2 已就利害關係人進行初步識別與類型分類，包含內部相關部門(如研發、品保、客服、法務等)、使用者、合作夥伴、供應鏈廠商與通報機構(TWCERT/CC)等類型。在實際處理漏洞事件時，PSIRT 應依漏洞風險等級、受影響產品範圍及事件的公眾關注度，進一步判斷需通知之利害關係人對象，並依據通報急迫性進行優先順序排序。

對於尚未確認之漏洞，宜先與內部關鍵單位(如資訊安全部門、產品開發部門等)進行討論與預備溝通，待確認後再依需求對外部利害關係人進行通報與溝通，以確保資訊正確且一致，並減少誤解或不必要的信任損耗。

●溝通時機與節點

漏洞處理過程中，妥善掌握關鍵時機進行利害關係人溝通，有助於風險管控、信任維持與聲譽管理。PSIRT 應根據事件進展，主動進行資訊溝通或通報。透過系統性掌握以下溝通節點，PSIRT 能強化事件透明度與管理效率，亦有助於利害關係人即時因應與風險降低。

– 確認漏洞已成立

當漏洞經初步驗證認為有效且對產品造成實質風險時，應即時通知相

關內部單位(如資安部門、產品開發、客服等)進入因應準備程序；若漏洞由外部通報者提出，亦應依通報政策進行回應。

– 制定修補時程

當修補方案已評估可行且制定明確時程後，應告知必要利害關係人(如客服單位、顧客代表等)，以利預先應對可能的查詢與支援準備。

– 修補釋出前後

釋出前，應預先通知受影響客戶與合作夥伴，說明預計發布時間與更新內容；釋出後，則應該主動提供更新公告與適用版本資訊，協助用戶完成更新。

– 若無法立即修補

雖然漏洞已確認，但因技術限制或其他考量無法立即修補，應主動提供暫時性緩解措施，並說明預計修補時程與影響，以維持外部信任與內部一致預期。

– 若出現風險外洩疑慮

如發現漏洞細節可能外洩、已遭利用，或媒體報導等公開資訊浮現，PSIRT 應立即依應變政策通報相關主管單位與利害關係人，必要時主動發布預警與澄清訊息，減少潛在誤解與損害。

●溝通內容與格式

PSIRT 在執行漏洞通報與修補相關溝通作業時，應建立清楚的溝通內容模板，以確保資料的完整性與風險控管專業性。

溝通內容應依利害關係人類型調整細節程度與措辭風格，可區分為內部通知與外部公告這二種主要範疇：

– 內部溝通

對於內部通知，PSIRT 應針對各相關部門進行精準傳達，包括產品研發、客服、維運、行銷與法務等部門。此類通知可涵蓋較多的技術細節，例如漏洞成因分析、修補時程規劃與緩解步驟，目的在於促進部門間的即時協作與整體應變效率。同時，內部通知亦能作為啟動外部公告準備工作的前置溝通機制，確保後續對外發布資訊的一致性與準確性。此外，當漏洞通報或相關資訊被標示為 TLP 分級時，PSIRT 應嚴格遵循其資訊分享規範。

– 外部公告

對於外部公告，則需根據目標受眾的資訊接受能力與敏感性，進行適度調整。主要對象包含終端用戶、合作夥伴、開源社群及媒體等。公告內容應避免揭露過多技術細節，轉而聚焦於漏洞影響說明、可採取的行動建議與修補更新資訊，協助使用者快速評估自身風險與採取防護措施。妥善的對外公告不僅有助於降低資安事件造成的實際損害，也能維繫組織品牌信任與公開透明的形象。

無論內部或外部利害關係人通知，為了避免資訊落差與誤解，建議可依照下列核心資訊，作為標準通報內容要素。此外，建議公告內容可多國語言撰寫，以利國內外用戶理解。

– 漏洞識別資訊：CVE 編號、漏洞名稱、漏洞描述摘要，如有內部漏洞編號可自行新增。

– 影響範圍：列出受影響之產品型號、版本範圍、部署場景(如地端、雲端)。

– 風險等級與說明：引用 CVSS 分數、TLP 分級、攻擊路徑等資訊，並簡要說明潛在風險。

– 修補狀態與更新資訊：是否已完成修補、可用版本、更新方式以及下載路徑。

– 緩解措施(若修補尚未完成)：建議短期風險降低方法。

– 聯絡方式：提供 PSIRT 窗口或技術支援資訊，方便後續查詢或反饋。

PSIRT 建立完整的溝通內容模板，除發布人類可讀(Human-readable)安全公告的外，應逐步導入 CSAF (Common Security Advisory Framework)與 VEX (Vulnerability Exploitability Exchange)等機器可讀(Machine-readable)格式。

此舉旨在透過精確的組件識別碼(如 PURL/CPE)銜接產品之 SBOM，協助下游客戶利用自動化工具進行快速比對，精確掌握產品真實受影響程度(而非僅依據元件名稱產生誤判)。透過導入 CSAF 與 VEX 聲明，PSIRT 能有效排除無效誤報並提供即時修復指引，從而提升風險管控的專業性，並大幅強化供應鏈漏洞處置的效率與透明度。

●溝通管道與責任分工

為確保漏洞資訊能即時且準確傳達給各類利害關係人，PSIRT 應建立明確的溝通管道與責任分工機制，涵蓋內外部溝通情境，並考量不同對象之資訊需求與時效要求。

在溝通管道規劃方面，建議組織應建立多元且具冗餘性的通訊機制，包括但不限於電子郵件(含具加密機制之 PGP 通訊)、內部通報系統、企業協作平台、客服回報系統、官方網站頁面及社群媒體。針對高敏感度或需加密傳輸之通報內容，應明確指定使用特定通道，以維護資訊機密性與完整性。

在責任分工方面，PSIRT 應明確劃分溝通任務之負責角色，例如：

– 技術內容撰寫

由 PSIRT 技術小組負責提供事件描述、影響範圍與修補建議。

– 溝通對象識別與發送清單確認

由 PSIRT 協調人或通報管理角色確認通知對象清單是否完整，並依據情境分層發送。

– 內部通報與部門協調

由 PSIRT 統整資訊後，透過主管層級或資訊安全負責人轉達內部相關單位(如客服、法務等)。

– 外部通報者應對與回覆

針對外部通報者或轉介單位(如 TWCERT/CC）所提出的漏洞報告，應指定專責人員回覆確認與處置狀態，並提供後續追蹤資訊。必要時可邀請其參與技術討論，增進合作關係與溝通透明度。

– 外部溝通與公告

由 PSIRT 配合公共關係或行銷單位共同審核內容後對外發布，確保資訊一致性並符合法遵需求。

– 重大事件升級通報

若事件涉及重大營運風險或須向主管機關通報，應由資安長或其授權人員審核並親自負責處理。

整體溝通流程應建立 SOP，並於演練中實際模擬，以確保在事件發生時，資訊能迅速傳遞，相關人員各司其職，不致錯漏。

3.2.7 資訊公開原則

完成漏洞修補或確認可提供緩解措施後，PSIRT 應依據既定政策適時對外發布資訊公告，維護用戶權益與產品信任。同時透過一致且專業的揭露機制，展現組織對於資安事件透明處理的承諾，促進利害關係人溝通與風險降低。

●漏洞揭露政策與原則

組織應遵循「負責任揭露(Responsible Disclosure)」原則，並建立明確的揭露條件與時機點。一般建議於完成漏洞修補、或已提供有效緩解措施後進行揭露。若屬重大風險或涉及廣泛影響，亦可考量與通報者協調揭露時間，兼顧修補完成與風險控管。

●致謝與公開表揚

對協助揭露漏洞的通報者，組織應建立致謝機制，如安全公告中列名、頒發電子感謝證書、邀請參與獎勵計畫等。此舉除鼓勵負責任通報行為，也能強化組織的資安正面形象。

如組織願意進一步表達資安重視，也可將漏洞揭露處理統計納入年度報告或企業永續計畫書(ESG/CSR)，展現治理透明度與資安治理成熟度。

3.3 查核階段(Check)

在 PSIRT 制度實施一段期間後，組織應進入查核階段，針對既有流程與實際運作成效進行系統性評估。本階段旨在確認漏洞處理各環節是否遵循既定政策與標準作業程序，並藉由資料彙整、跨部門回饋與實務觀察，識別流程中的瓶頸與偏差，作為後續機制精進的重要依據。查核作業不僅有助於強化組織內部治理機制，亦能提升通報處理流程的透明度與一致性。本章節將從以下四個面向(詳見圖 10)，說明查核階段應執行之具體作法與評估重點。

資料來源：TWCERT/CC 整理

圖10 PSIRT 查核階段

3.3.1 案例彙整與分析

為持續強化漏洞對應機制，PSIRT 應定期彙整與分析歷來之漏洞通報案例，從中掌握趨勢脈絡與系統性問題，進而作為提升資安管理能量的重要依據。此項作業不僅有助於回顧應變效能，亦有利於資安教育資源的聚焦、產品資安設計的改進與組織整體風險意識的提升。

●漏洞通報案例分類與統計

PSIRT 應建立標準化的分類架構，建議將已處理之事件依據不同維度進行彙整與統計，包括：漏洞技術類型(參考 3.2.4)、)、通報來源類型(參考 3.2.2)、產品分類(參考 3.2.4)、)與漏洞影響範圍與風險等級(參考 3.2.4)。藉由系統性歸納，可提升漏洞管理的整體可視性與後續強化作業的依據性。

PSIRT 可透過定期統計分析產出趨勢報告，以識別特定產品、模組或漏洞類型中潛藏的高風險區域，或發掘組織內重複發生的常見弱點，進而提出改善建議與策略。

此外，分析結果亦可作為資安教育訓練與系統開發準則制定的參考依據。例如，若統計顯示某類型漏洞頻繁出現，PSIRT 可建議資安單位規劃專門課程，並將其納入新進開發人員訓練內容。此外，若某產品多次因類似設計缺陷導致資安弱點，則可與開發團隊共同檢視其開發與測試流程，評估是否引入自動化檢測機制或加強設計階段的安全審查，以降低重複錯誤發生的風險。

●處理時效與風險分級成效分析

PSIRT 亦可針對過去漏洞依其風險等級，統計實際處理與修補所需時間，並與內部設定之處置時效進行比對分析。若出現處置超時的情況，應調查原因並記錄影響因素，如資源不足、第三方依賴延遲，或內部流程瓶頸等，作為未來調整政策或精進流程的參考。

3.3.2 流程檢視與評估

為確保 PSIRT 實際運作是否與 SOP 一致，並維持處理流程的可預期性與透明度，組織應定期執行 PSIRT 作業流程之符合性評估。此評估作業應涵蓋流程步驟執行情況、文件記錄完整性，以及異常處理之風險管控，藉以強化制度落實與持續改善基礎。

●作業流程比對與執行紀錄查核

PSIRT 應針對已處理之漏洞案例，逐一比對其處理流程是否符合原先規劃之各項作業節點，例如：

– 是否依通報流程建立紀錄

– 是否按流程完成漏洞確認、風險評估、修補決策與公告

– 是否如期完成修補、功能測試與利害關係人通知

透過流程紀錄比對，可識別流程中可能發生的延遲、遺漏或執行落差，

並進一步分析其成因，如人力資源不足、交接不清、缺乏指引等。

●作業紀錄完整性與透明度檢查

除了作業流程本身外，PSIRT 亦應定期檢視各項處理紀錄是否具備完整性與可追溯性，並符合資訊揭露之相關要求。這些紀錄應包括通報案件之編號與登記時間、風險評估與決策依據、修補實施與測試報告，以及對內對外溝通文件等。透過強化紀錄透明度，能提升審核與稽核機制的有效性，日後若發生資安風險爭議時，提供可供溯源與檢討的依據，確保處置過程之正當性與可受公評性。

●異常流程與例外處理的控管

在實務運作上，漏洞處理過程中可能因特殊情境(如無法重現、第三方延遲修補、以緩解措施替代修補等)而採取與標準流程不同的處置方式。對此，PSIRT 應確實記錄偏離處置的原因、決策依據與通報對象，並進一步評估是否反映制度缺口或流程盲點，必要時可強化相關指引或調整資源配置。最終，所有偏離案例皆應納入後續風險控管機制與教育訓練教材中，作為組織持續改善的依據。

若異常流程偏離既有 SOP 的情況頻繁或比例過高，應由 PSIRT 發起制度檢討作業，研議是否需調整 SOP，使其更貼近實務情境，並保有足夠應變彈性。制度與流程設計應兼顧標準性與實務適用性，避免過於僵化而造成作業低效與溝通障礙。

3.3.3 跨部門合作檢視

漏洞事件處理通常涉及多個部門共同協作，包括研發、維運、客服與行銷等。為確保 PSIRT 作業流程的有效運作與持續精進，建議定期檢視跨部門合作的溝通紀錄與協作狀況，作為組織流程健全度與應變能力的評估依據。

●溝通紀錄與會議彙整

審查漏洞處理過程中，應確認是否留存足夠的跨部門協作與會議紀錄，包括通報接收後招開的緊急會議、修補時程協調、公告內容討論等。透過彙整與回顧相關會議記錄與聯繫過程，有助於掌握關鍵協作節點的運作是否順暢，並提早辨識潛在風險。審查時應特別留意是否曾出現以下情形：

– 跨部門間溝通斷點，導致資訊遺漏或錯誤傳達

– 決策共識不足，影響時效或處置一致性

– 因部門權責認知不清而產生爭議或延遲

透過上述檢視，可作為精進協作流程與角色釐清的重要依據。

●資源協調與人力調度情形

查核漏洞處理過程中，應評估各支援部門在不同階段的應變效率與投入程度，例如：修補階段能否即時取得研發資源進行修正、用戶回應階段是否有客服或法務人員支援說明撰寫與回應、公告發布前是否獲得行銷與品牌部門的協調配合。針對協作過程中出現的人力資源不足、部門配合延遲等情形，應予以紀錄與分析，並研議是否需建立資源調度機制或設定明確的跨部門協作時限，以提升整體應變效率。

●問題回饋與跨部門改善建議

各部門於漏洞處理過程中的實務經驗與意見，應定期彙整作為 PSIRT 制度調整的重要依據。建議透過匿名問卷、定期協調會議或事件回顧報告等方式，蒐集各單位對流程設計、責任分工、溝通機制等面向的回饋，例如流程是否過於繁瑣、分工是否合理、回應節奏是否符合實務需求。對於具有重複性或共通性的建議，應納入流程改進計畫，以持續強化制

度運作與跨部門協作效能。

3.3.4 通報者關係管理

通報者是產品安全維護中極具價值的外部合作力量，尤其對於能持續提出高品質、具建設性意見的通報者，應視為長期合作的夥伴資源。透過系統化識別與管理機制，組織可強化與通報者的信任關係，建議穩定合作模式，進一步提升漏洞通報的效率與產品整體安全水準。

●建立通報者識別與資料維護

為確保溝通效率與合作潛力辨識，建議針對曾進行通報者建立識別紀錄，包含通報頻率、通報內容正確性、回應配合度、專長領域(如 Web 應用、系統弱點等)等資料。透過分析通報者的技術傾向與通報紀錄，PSIRT 可進一步判斷其是否具備合作潛力，或是否可納入後續測試邀請、研討活動等合作名單。

●維運長期合作通報者名單

建議建立定期維護之「活躍通報者名單」，記錄其聯繫方式、偏好溝通管道(如 Email、漏洞回報平台、加密通訊等)，並定期驗證聯繫資訊正確性。除基礎聯絡資訊外，也應評估通報品質與回應時效，辨識出通報者中之核心合作對象，必要時可比照合作廠商等級進行分類管理。

●發展合作機制與參與方式

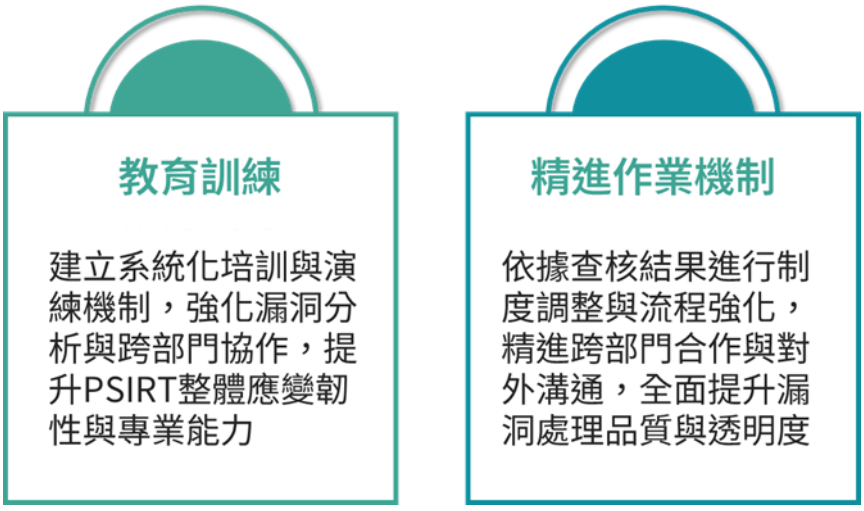
對於具備高配合度與專業能力之通報者，可依組織資安政策發展更進一步的合作機制。例如，在產品正式發佈前，選擇性邀請信任通報者參與預先發行測試(Pre-release Testing)，透過實際操作進行漏洞挖掘與預警，協助組織在產品上線前即完成修補與風險降低，有效縮減上市後修補的時間與成本。

●回饋與關係維繫

為強化通報者參與意願與長期合作關係，可建立多元回饋機制。例如設立名人堂公開表揚對產品安全具重大貢獻者，或提供專屬的聯繫窗口與快速回應通道，讓通報者感受被組織重視。必要時也可考慮發放證書、邀請參與內部活動，或提供其他非金錢性質的肯定方式，深化合作夥伴關係。

3.4 改善階段(Act)

在完成查核與評估後，PSIRT 應進入改善階段，針對前一階段所揭露的問題與潛在風險，規劃並落實具體的改善行動。本階段核心在於持續強化團隊能力與制度機制，以提升漏洞處理效能與跨部門協作品質。透過定期培訓、演練機制建立、作業流程改善與成效指標監控，組織將能逐步提升 PSIRT 的應變成熟度與資安治理水準。本章節將從「教育訓練」與「精進作業機制」兩個面向進行說明，詳見圖 11。



資料來源：TWCERT/CC 整理

圖11 PSIRT 改善階段

3.4.1 教育訓練

為確保 PSIRT 成員具備充足的專業能力與應變素質，組織應制定系統化的培訓與演練機制。此機制不僅有助於強化技術層面的漏洞分析與處置能力，也能促進跨部門協作與危機溝通效率，進而提升整體資安應變韌性。唯有將能力培育納入日常管理與長期規劃，方能建立一支具備韌性與前瞻性的 PSIRT 團隊，持續應對快速變化的資安威脅環境。

●培訓需求分析與課程設計

建議可依據 3.3.1 進行培訓需求分析，透過統計數據掌握組織產品在安全設計與開發上的能力缺口，據以設計針對性課程內容。課程可涵蓋技術技能(如漏洞分析工具使用、修補策略實務)與流程教育(如通報回應流程、法規遵循事項)，以系統性方式強化團隊在實務作業中所需之專業知識與應變能力，提升整體資安事件處置效能。

●整合內部與外部培訓資源

組織應整合內外部培訓資源，建立完善且具延續性的培訓資源體系。除安排內部定期教育訓練，亦可鼓勵成員參與外部專業研討會、技術社群交流與相關證照課程，強化實務知能與趨勢掌握。同時，建議建置集中管理的培訓教材資源庫，提供標準化學習素材與歷年課程內容，供成員隨時查閱與進修，促進知識傳承、降低新人學習曲線，並強化整體組織資安應變能量。

●演練計畫與模擬測試

在演練規劃方面，應設計貼近實務操作的模擬測試情境，涵蓋漏洞通報接收與分類、跨部門協調處置、利害關係人溝通應對、修補版本發布與公告等核心流程。透過定期演練，不僅可驗證 PSIRT 團隊在實際應變中的協作能力與處置效率，亦有助於發掘流程設計的潛在盲點與作業瓶

頸，作為制度調整的依據。演練結束後，應召開檢討會議，全面回顧演練中流程運作與成員表現，進行差異分析並提出具體改善建議，以強化後續事件處理之整體應變成熟度。

●培訓成效評估與持續改進

建議組織建立系統化的成效評估機制，透過測驗、實作觀察、匿名問卷回饋等多元方式，定期檢視培訓與演練的實際成效。評估結果可用以辨識學習成效差距與課程設計盲點，並據此調整後續課程規劃與演練內容，確保訓練資源投資與人員能力發展間的連結性，推動持續改進與整體資安應變效能的提升。

3.4.2 精進作業機制

為持續強化 PSIRT 的運作效能，組織應根據查核階段所揭露的問題與建議，進行整體作業機制之精進。本階段聚焦於制度流程調整、跨部門合作強化、對外溝通機制調整及成效監控機制建置，藉此全面提升漏洞處理的品質、效率與透明度。

●流程調整與制度完善

應針對查核階段所揭露的制度瓶頸進行檢討與調整。檢討內容可涵蓋漏洞通報機制、修補與測試流程、公告揭露節點等，釐清是否存在過於繁瑣、責任不明或權限配置不當的情形。修正後的流程應同步更新內部作業文件與標準作業程序(SOP)，並搭配教育訓練以強化人員執行力。

●跨部門協作強化

在跨部門協作方面，建議建立定期協調機制，例如月會或專案會議，針對重大漏洞事件進行橫向資訊共享與資源整合。同時，可重新盤點流程中各角色的參與時機與責任分工，調整角色界面與任務指派，使合作過程更順暢、責任更明確，有助於降低溝通摩擦與時效延誤。

●對外通報流程機制精進

對外通報流程亦需持續精進，建議檢視通報者溝通與回應機制，包括回應時效、內容完整性、回饋流程是否清楚，提升通報者整體互動體驗。在資安公告部分，應精進審查制度，明確規劃公告草擬、審核、發布各階段節點與負責單位，並考量當前用戶常用的社群與媒體平台，調整資訊公告方式。同時，建議定期盤點外部利害關係人聯繫窗口的正確性與通報管道的可用性，以確保外部溝通不中斷。

●成效監控與關鍵績效指標(KPI)

導入成效監控機制與關鍵績效指標(KPI)，如漏洞平均處理時間、回應時間、公告時效與通報品質指標等。透過數據持續監控 PSIRT 作業成果，並定期召開檢視會議，調整目標與策略，以達成流程最佳化與組織整體資安韌性的提升。

4. PSIRT 導入建議

考量企業在產品供應鏈中扮演的角色多元(如製造商、代理商、系統整合商等)，其對產品設計與原始碼的掌控力及資源配置亦不盡相同，PSIRT 的發展應秉持因地制宜的原則，針對組織特性提供客製化的導入策略。

考量企業在各發展階段的資安成熟度差異，本手冊在 PDCA 架構下，提供循序漸進的實務指引。建議企業依自身角色與能力，將導入歷程劃分為初階、進階、高階等三個階段：由建立漏洞揭露機制(VDP)做為起點，確保漏洞能有效接收；隨後逐步強化制度化流程與跨部門協作；最終隨經驗成熟成立專屬 PSIRT。透過這種彈性且可持續的發展模式，企業能兼顧可行性與治理水準，將漏洞管理內化為企業治理的核心(詳見圖 12)。

資料來源：TWCERT/CC 整理

圖12 PSIRT 三階段

4.1 企業角色與界定

導入 PSIRT 或相關機制前，企業應先明確界定自身於產品供應鏈中的角色與責任範圍。並非所有企業皆具備直接修補產品漏洞的能力，例如代理商或經銷商通常無法存取原始程式碼，亦無權決定修補內容與時程；系統整

合商則可能僅能針對整合層或部署環境提出緩解建議。在此情況下，企業並非無法履行產品安全責任，而是其責任重點應放在漏洞資訊的接收、初步影響研判、通報轉介原廠，以及與客戶或利害關係人之溝通協調。透過清楚界定責任歸屬，有助於避免制度流於形式，並確保漏洞處理作業符合實際運作情境。

4.2 PSIRT 建置階段

在 PSIRT 建置的初階階段，企業尚未成立專責 PSIRT 組織，以 Plan(規劃)與 Do(執行)為核心，建立可實際運作的基礎機制。規劃階段以指定產品安全事件之負責窗口為主，並確認企業現階段可提供之最基本 PSIRT 服務項目，針對資源有限之企業，建議採行「跨部門任務編組」模式，無需立即成立專責部門，而是由研發主管、法務代表、品保(QA)組成核心小組，優先以建立「漏洞揭露機制(Vulnerability Disclosure Program, VDP)」為重點，同時訂定最低限度之作業原則，包含漏洞通報之接收方式、初步處理流程及回應原則。此模式能以最低成本滿足供應鏈對安全透明度的基本要求，並確保企業具備初步的風險對接能力。

執行階段則透過設置單一且明確之漏洞通報管道(如專用電子郵件或線上表單)，平時由專人定期檢視通報資訊，進行漏洞資訊之接收、基本分類及內部通報流程，並對通報者提供基本回覆與溝通機制，確保企業具備漏洞通報之接收與回應能力，作為後續 PSIRT 制度化建置之基礎(詳見圖 13)

資料來源：TWCERT/CC 整理

圖13 初階階段漏洞處理流程

在 PSIRT 建置的進階階段，企業已具備基本漏洞通報與回應能力，導入重點由個案處理轉為制度化之漏洞管理，並使 Plan、Do、Check 三個階段開始全面運作。規劃階段著重於明確 PSIRT 成員小組之組成，得採跨部門方式運作，並建立責任分工機制(如 RACI)，同時訂定一致之漏洞分級與修補原則；執行階段則將漏洞通報、分類、評估與修補等作業流程予以標準化，並建立專屬之溝通管道與案件紀錄機制，依據風險等級進行修補優先順序之管理；查核階段開始針對漏洞處理案例進行彙整與分析，檢視作業流程之順暢性、跨部門協作情形，以及對通報者與內部單位之溝通品質，以確保漏洞處理流程具備可追蹤、可檢視與可改善之管理特性，作為邁向成熟 PSIRT 機制之關鍵階段。

在 PSIRT 建置的高階階段，企業已完成制度化漏洞管理，並進一步將 PSIRT 納入組織治理與產品生命週期管理，使 Plan、Do、Check、Act 形成持續運作之循環機制。規劃階段著重於正式建立專屬 PSIRT 組織與治理架構，明確其角色定位與服務範疇，並將產品安全風險管理納入組織既有管理體系；執行階段則透過流程自動化與工具化，強化漏洞管理效率，並深化與外部利害關係人(如研究社群、CERT 或供應鏈夥伴)之協作，並積極申請成為 CVE 編號管理者(CNA)，掌握產品漏洞之定義權與發布時程主導性，展現國際級的資安治理成熟度與當責態度；查核階段除持續追蹤漏洞處理績效外，進一步進行跨產品與跨版本之漏洞趨勢與根因分析；改善階段則依據檢視結果持續精進作業機制、教育訓練與內部流程，並將經驗回饋至產品設計與開發流程，促使 PSIRT 成為支撐企業產品安全與風險治理之長期運作機制。

5. 參考準則與法規

為確保 PSIRT 制度之建置與運作具備國際一致性、產業適用性與法規遵循，組織推動產品資安事件回應機制時，應全面參照相關標準規範與法令要求。本章節彙整 PSIRT 建置實務中常見之國際標準、主要國家或區域的法規要求，並涵蓋特定產業領域的安全準則。透過這些規範的掌握與應用，不僅可提升 PSIRT 作業的正當性與可稽核性，亦有助於強化組織在全球市場中的信任度與競爭力。

5.1 參考指南與國際標準

為保障 PSIRT 作業與國際實務接軌，組織在規劃與建置階段應參考相關國際標準作為制度設計與流程規劃的依據。這些標準不僅提供漏洞通報與應變流程的指引，亦有助於組織強化資訊安全治理、風險管理與對外溝通能力。以下分成「服務架構與運作準則」與「產品安全事件處理流程」兩種類別說明。

●服務架構與運作準則

– FSIRT Service Framework[1]

由全球知名資安事件協調組織 FIRST 發布的產品安全事件應變團隊建置框架。此框架適用於負責產品安全事件回應的企業或組織，特別是開發並銷售具數位功能產品的製造商與供應商。此文件包含清晰的通報流程、定義事件分類與處理階段、確保跨部門合作，以及維護通報者關係與公開揭露政策。此外，亦提供 PSIRT 在建立服務範圍、作業流程與角色職責分工上的指南，有助於確保事件應變具一致性、透明度與可預期性，並與國際通行做法接軌。

– Security Incident Management Maturity Model, Version 2(SIM3 v2)[7]

由 Open CSIRT Foundation 推出的資安事件管理成熟度模型，旨在提供

CSIRT 用以衡量與提升事件管理能力的評量工具。雖然 SIM3 原為 CSIRT 設計，但其架構與核心原則同樣適用於 PSIRT 制度之規劃，特別是面對日益複雜的產品漏洞管理需求，PSIRT 可參考 SIM3 的分類與評分機制，釐清組織責任、建立處理流程與衡量成熟度，不僅有助於對標國際慣例，也能強化組織在處理產品安全事件時的回應能力與治理透明度。

●產品安全事件處理流程

– ISO/IEC 30111[8]

ISO/IEC 30111 是針對資訊與通訊技術產品所制定的漏洞處理流程標準，適用於開發或維護軟體、韌體與硬體產品的製造商與供應商。該標準規範從漏洞接收、驗證、分析、修補至結案的完整處理程序，並強調需設立明確的責任分工與跨部門協作機制。對 PSIRT 而言，ISO/IEC 30111 是建立內部漏洞應變作業流程的核心依據，可協助團隊有效管理外部通報或內部發現的產品弱點，並確保應對流程具一致性、可追溯性與風險導向。此標準亦與 ISO/IEC 29147[9]相輔相成，共同支撐組織的產品安全事件處理能力。

– ISO/IEC 29147[9]

ISO/IEC 29147 是專為漏洞揭露所制定的國際標準，適用於產品供應商、系統整合商與服務提供者等需處理外部通報漏洞的組織。該標準主要規範如何建立公開、可信賴的漏洞通報機制，包含通報管道設置、回應政策、通報人致謝與資訊公開原則。對 PSIRT 而言，ISO/IEC 29147 提供建立與通報者互動及揭露策略的參考依據，是制定通報政策、外部溝通流程及協調揭露時程的關鍵準則，並與 ISO/IEC 30111 互相補強[8]，共同構成產品弱點管理的國際標準實踐。

●治理與管理框架

– ISO/IEC 27001

ISO/IEC 27001，其名稱是《資訊科技-安全技術-資訊安全管理系統-要求》(Information technology-Security techniques-Information security management systems -Requirements），為國際標準化組織制定的資訊安全管理系統標準，適用於希望系統性管理資訊風險的各類型組織。此標準強調透過風險評估與控制措施，保障資訊的機密性、完整性與可用性，其要求涵蓋資安政策制定、資產管理、存取控制、事故應變與持續改進機制。對 PSIRT 而言，ISO/IEC 27001 提供制度化資安事件管理基礎，有助於 PSIRT 與組織整體資安治理相銜接，並確保事件通報、調查與修補行動均符合風險控管與稽核要求，提升整體應變效能與可信度。

– ISO 31000

ISO 31000 是國際標準化組織發布的風險管理指導標準，適用於各行各業與各類組織。該標準提供系統化的風險管理框架與流程，協助組織有效識別、評估、處理及監控風險，以達成既定目標並提升決策品質。雖然 ISO 31000 並非專門針對產品漏洞處理所設計，仍可作為 PSIRT 建立漏洞處置流程與決策準則的重要參考。藉由整合整體風險管理機制，該標準有助強化產品安全事件的風險評估與優先處理，促進跨部門協作與持續改進，進一步提升事件回應的效率與效果。

以上標準雖涵蓋面向不同，但皆對 PSIRT 建立與運作提供具體且可操作的參考，亦為企業因應全球供應鏈資安要求、符合法規遵循與提升品牌信任的關鍵依據。

5.2 各國與地區法規要求

不同國家與地區對於產品漏洞處理的合規要求日益明確，PSIRT 應依據組織營運地區與產品銷售市場，參考相關資安與責任揭露規範，以下將以美國、歐盟與英國為例說明。

●美國相關法規與指導

– 安全設計(Secure by Design)[11]

Secure by Design 由 CISA、美國國內組織和國際合作夥伴聯合發布，源自軟體與產品開發領域的安全設計原則。並獲多國政府積極推廣，適用於所有設計、開發與提供具數位功能產品的廠商。其核心理念是在產品設計初期即納入安全考量，確保資安機制內建於產品生命週期中，而非事後補救。最新版指南整合數百名利害關係人的回饋，擴展三大原則：對客戶安全結果負責、強化透明與問責制、落實自上而下的資安領導。對 PSIRT 而言 Secure by Design 有助於降低弱點數量與嚴重程度，促進與開發團隊協作，強化漏洞回應流程與回饋機制，建立以預防為核心的產品安全文化。

– Secure by Demand Guide[12]

由美國 CISA 所發布的資安採購指引，適用於一般企業、政府機關及關鍵基礎建設等採購具有數位功能產品與服務的組織。該指南強調資安要求應貫穿採購前、中、後全流程，並與 Secure by Design 原則相輔相成。採購前透過資安提問了解廠商的安全設計與應變能力；採購階段則將產品安全要求納入合約條款，強化供應商責任；採購後持續評估產品的安全性。對 PSIRT 而言，此指引促進供應商建立正式的通報與處理流程，並作為回應買方資安要求與建立信任的依據，進一步強化供應鏈資安透明度與事件回應能力。

– 物聯網網路安全法(IoT Cybersecurity Improvement Act)[13]

IoT Cybersecurity Improvement Act 是美國於 2020 年通過的物聯網資安法規，其規範主體為聯邦政府各機關，旨在透過政府採購與使用政策，推動 IoT 裝置之資安要求，藉此間接影響向聯邦政府提供 IoT 裝置的製造商與承包商。由 NIST 擔任標準制定單位，定期發布與更新最低資安要求。此法強調供應商須具備通報與應變機制，確保弱點能即時被接收、分析與修補，並與政府機關溝通補救進度。

– U.S Cyber Trust Mark[14]

由美國聯邦通訊委員會（Federal Communications Commission，FCC）於 2025 年啟動，適用於銷售至美國市場的消費性無線智慧家居等 IoT 產品，如相機、監視器、智能音箱、健身追蹤器等消費性網路裝置。若要獲得 Cyber Trust Mark 標章的產品，必須符合 NIST 提出的資安規範標準，涵蓋預設使用強密碼、資料保護、軟體或韌體更新和事故偵測能力等。

●歐盟相關法規與指導

– 網路韌性法案(Cyber Resilience Act, CRA)[15]

CRA 為歐盟於 2024 年通過的資安法規，適用於歐盟市場銷售具有數位元素產品的製造商、進口商與經銷商，不論產品是否於歐盟境內製造，只要在歐盟市場上市，即須遵守該規範。該法要求產品在整個生命週期內維持產品安全性，涵蓋設計時的風險管理、漏洞管理能力、事件通報義務、修補時效與安全更新年限等。

– NIS2 Directive[16]

NIS2 Directive 是歐盟於 2023 年生效的資安指令，擴大 2016 年實施的 NIS Directive 所規範的類別與規模，例如：公共電子通訊網路或服務

供應、特定關鍵產品、社交平台等，並以企業規模進行區分，中大型企業皆須遵守 NIS2 Directive 之規定。此外，NIS2 Directive 具有為詳細且具體之要求，如實施風險管理措施、弱點處理與揭露、資安事件通報、營運持續機制與供應鏈資安管理。

●英國相關法規

– 產品安全和電信基礎設施法案(Product Security and Telecommunications Infrastructure, PSTI)[17]

PSTI 是英國於 2023 年通過的產品資安法案，適用於銷售、進口貨製造連網消費性產品的業者，如 IoT 裝置、智慧家電、連網手機等。此法要求產品具備基本資安能力，涵蓋禁止廠商出廠設置通用密碼、建立漏洞通報機制，以及明示產品的資安支援年限。

5.3 產業特殊規範

依照產品所屬產業性質，不同產業也制定特定的資安漏洞管理規範。PSIRT 在建置時應考量適用產業的標準需求，例如：

●醫療產業

– U.S. FDA-Cybersecurity in Medical Devices[18]

此為美國食品藥物管理局(FDA)發布之資安指引，適用於設計、製造與銷售連網醫療設備的製造商，其產品包含但不限於醫療器材產品其組成包含軟體(韌體)、具有可程式邏輯裝置、醫療器材軟體(包括行動應用程式)。指南強調廠商須於產品生命週期早期即導入資安風險管理機制，亦要求業者提交包含第三方與開源元件的軟體物料清單(SBOM)。此外，也強調透明揭露、標示資訊與第三方元件風險管理，確保使用者可妥善維護裝置資訊安全。

●OT 場域

– NIST 800-82[19]

由 NIST 發布，針對工業控制與各類操作技術環境提供系統性的資安建議。文件涵蓋 OT 架構設計、風險管理、事件應變、網路隔離與防禦等實務措施，廣泛適用於能源、製造、水資源、交通等關鍵基礎設施領域。此外，對安全設計、持續監控、修復能力與跨部門協作要求，亦可作為建置 PSIRT 時的重要參考，有助於提升產品在實體環境中的安全性與韌性。

●IoT 領域

– NIST IR 8259[20]

此指導文件由 NIST 所發布的指導文件，旨在為物聯網設備製造商提供一套基礎的網路安全活動與核心安全能力基準線。該指南強調物聯網設備在設計、開發和上市前，應具備身分驗證、數據保護、軟體更新管理等基本安全功能，以減少安全風險並提升用戶信任。該文件不僅協助製造商建立安全框架，還推廣物聯網產業標準化，提升整體物聯網環境安全性。

●無線電設備

– 歐盟-Radio Equipment Directive(RED)[21]

該指令適用於歐盟及歐洲經濟區市場銷售的無線電設備，產品涵蓋 Wi-Fi、藍牙、行動電話等多種無線設備，規範設備必須符合健康與安全保護、電磁相容性及無線電頻譜有效利用等基本要求，確保產品不會對使用者及其他人造成危害，且避免有害干擾。另外，RED 於 2025 年 8 月起，強制實施更嚴格的網路安全要求，包含防止設備損害網路、保護個人數據與隱私、防止詐欺等。

– EN 18031

EN 18031 是歐盟為配合 RED 指令所新增的協調標準，專注於無線電設備的網路安全要求。此標準是由歐洲標準委員會(CEN)和電工委員會(CENELEC)聯合制定，主要分防止網路損害與服務退化、保護個人數據和用戶隱私、及防止處理虛擬貨幣的無線設備詐欺的措施三個部分。此外，EN 18031 的納入，在無線電設備網路安全領域，為製造商提供明確的技術指引，並簡化合規流程。

6. 結論

在數位轉型與全球供應鏈高度連動的時代，產品安全事件的風險逐漸成為企業營運與品牌信任的重要挑戰。面對日益頻繁且複雜的漏洞通報，建立具備制度化運作能力的產品安全事件應變小組(PSIRT)，已成為企業提升資安治理成熟度的關鍵策略之一。

考量不同組織在規模、產品型態與資源配置上皆有所差異，PSIRT 並無唯一標準架構可循。因此，本手冊彙整常見 PSIRT 組織模型(集中式、分散式與混合式)與人員職責配置方式，說明其適用條件與發展彈性。無論採取何種模式，唯有明確責任、強化橫向協作與建立標準化流程，方能提升應變效率與溝通品質，確保產品資安事件的妥善處理。

在建置面向上，本手冊依循 PDCA 循環，分別就規劃、執行、查核與改善四階段說明具體作法。從確認服務內容與責任分配、建立通報處理流程、實施公告揭露與修補作業、直至跨部門協作與成效評估，各階段皆強調可落實性與資料導向原則。透過持續運作與機制調整，可強化漏洞處理流程的即時性與透明度，並逐步建構具備韌性與持續精進能力的 PSIRT 運作體系。

為確保 PSIRT 制度符應國際實務與法規要求，組織應整合多項標準與規範作為建置依據。國際可參考 FIRST 框架、ISO 系列標準，建立制度化流程與治理機制；法規面則應關注美國、歐盟等地資安要求，如 Secure by Design、CRA 與 PSTI 等。另應依產業特性，參照醫療、OT、IoT 等領域規範。

然而，企業僅為內部使用而開發少量工具系統，且未涉及外部客戶或重大法規要求，則可以考慮用其他資安應變流程替代完整 PSIRT，若若產品或服務對外提供、涉及供應鏈安全責任、法規遵循(如 NIST, ENISA 等)，仍建議建立完善的 PSIRT，以強化企業的漏洞處理機制。

上述準則有助於確保作業合規、強化風險應對並提升整體信任。

7. 參考文獻

[1]PSIRT Services Framework, [線上].Available: https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1-1.

[2]Common Weakness Enumeration, [線上]. Available: https://cwe.mitre.org/.

[3]Common Vulnerability Scoring System SIG,[線上]. Available: https://www.first.org/cvss/

[4]MITRE ATT&CK, [線上]. Available: https://attack.mitre.org/.

[5]FIRST Standards Definitions and Usage Guidance -Version 1.0, [線上]. Available: https://www.first.org/tlp/v1/.

[6]FIRST Standards Definitions and Usage Guidance -Version 2.0, [線上]. Available: https://www.first.org/tlp/.

[7]SIM3 Model & References, [線上]. Available: https://opencsirt.org/csirt-maturity/sim3-and-references/.

[8]ISO/IEC 30111:2019, [線上]. Available: https://www.iso.org/standard/69725.html.

[9]ISO/IEC 29147:2018, [線上]. Available: https://www.iso.org/standard/72311.html.

[10]ISO 31000:2018, [線上]. Available: https://www.iso.org/standard/65694.html.

[11]Secure by Design, [線上]. Available: https://www.cisa.gov/securebydesign.

[12]Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem, [線上]. Available: https://www.cisa.gov/resources-tools/resources/secure-demand-guide.

[13]H.R.1668 - IoT Cybersecurity Improvement Act of 2020, [線上]. Available: https://www.congress.gov/bill/116th-congress/house-bill/1668.

[14]U.S. Cyber Trust Mark, [線上]. Available: https://www.fcc.gov/CyberTrustMark.

[15]Cyber Resilience Act, [線上]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[16]NIS2 Directive: new rules on cybersecurity of network and information systems, [線上]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[17]The UK Product Security and Telecommunications Infrastructure (Product Security) regime, [線上]. Available: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime.

[18]Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, [線上]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.

[19]NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security, [線上]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

[20]NISTIR 8259 Series, [線上]. Available: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series.

[21]Radio Equipment Directive (RED), [線上]. Available: https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en.

8. 附件

附件1 建立 PSIRT 檢核表

附件2 TWCERT/CC 漏洞通報及申請 CVE 流程