機場防災韌性機制與我國精進課題探討

Exploring Airport Disaster Resilience Mechanisms and Advancement Issues for Taiwan

運輸工程及海空運組 呂蕙美

研究期間：民國114年3~12月

摘　要

隨著全球極端氣候與天然災害增加、資安攻擊頻傳及航空營運複雜度提升，機場防災韌性(Disaster Resilience)已成為國際組織及各國航空主管機關關注的核心議題。為降低機場及相關基礎設施災害風險，建立機場防災能力及檢討防災韌性機制，以保護機場資產、維持運作、確保業務連續性並增進機場基礎設施永續性，確有其必要性及迫切性。

本研究回顧國際在機場防災韌性相關指導文件與案例，並分析我國機場現行制度，發現國際機場防災趨勢已由單純符合法規與事件應變，轉向以風險導向、跨系統治理及全生命週期韌性管理為核心。在氣候變遷、複合型災害及航空系統高度數位化趨勢下，機場災害風險日趨多元且具連鎖效應。我國雖已建立災害防救、營運持續計畫、資通安全及國家關鍵基礎設施等制度，但在韌性量化評估與決策支援方面仍有強化空間。未來宜建立制度化機場防災韌性評估機制，並納入投資決策、營運管理及跨關鍵基礎設施合作，以利提升我國整體機場防災韌性。相關研究成果可做為我國民航主管機關與桃園機場公司政策制定及投資規劃參用。

關鍵詞：

韌性、機場、防災

機場防災韌性機制與我國精進課題探討

一、緒論

機場屬於關鍵基礎設施(Critical Infrastructure)，是旅客與貨物運輸的核心節點，亦與其他關鍵基礎設施如電信、電力與自來水等有高度連結，且在災害與人道危機期間扮演重要生命線角色，能提供快速的移動支援，協助國家因應相關災害所造成的嚴重衝擊。因此任何災害導致上述服務中斷，都會對機場帶來重大損害，且可能進而對整體經濟產生深遠的負面影響。

根據 MarketsandMarkets 所發布的《2030 年機場產業未來展望》(Future of Airport Industry to 2030)報告〔1〕，全球機場投資預計將在 2040 年前大幅成長，從 2021 年的 2,000 億美元增至 2040 年的 2.4 兆美元，年複合成長率達 14.4%；國際機場協會(Airports Council International, ACI) 2021 年報告〔2〕亦預測，至 2040 年，全球機場資本投資總額將達 2.4 兆美元；ACI 的 2025 年《機場經濟報告》(Airport Economics Report)〔3〕也預測未來航空需求預期持續強勁(2043 年全球旅客量達 17.7 億人次，2053 年達 22.3 億人次)，全球機場需要進行大量基礎設施投資，估計到 2040 年約需投入 2.4 兆美元機場基礎建設，以支撐未來旅客成長及相關經濟活動。防災韌性基礎設施聯盟(Coalition for Disaster Resilient Infrastructure, CDRI[1])也指出，由於近年來極端氣候頻率增加、地震災害風險高漲與航空運輸系統日益複雜，使災害對機場之影響日益嚴峻。機場做為國家關鍵基礎設施，若未於所推動專案之生命週期各階段導入防災韌性措施，大量投資金額將使機場基礎設施面臨高度風險〔4〕。

機場防災韌性已成為提高國土安全性、交通運輸持續性與國際連通性的重要課題。為降低機場及相關基礎設施災害風險，建立機場防災能力及檢討防災韌性機制，以保護機場資產、維持其持續運作與業務連續性及增進機場長期基礎設施永續性，確有其必要性及迫切性。另外，綜整國內現行機場防災相關制度與實務，可發現我國機場防災管理仍以「法規遵循」與「單一事件應變」為主要導向，著重於是否具備應變計畫、是否完成法

[1] CDRI(防災韌性基礎設施聯盟)是一個由各國、聯合國(UN)機構、多邊開發銀行、私營部門和學術機構組成的國際聯盟，旨在致力提升關鍵基礎設施韌性，促進防災基礎設施建設風險管理、標準、融資和恢復機制領域的研究與創用。截至 2023 年，CDRI 已擁有 39 個成員國。

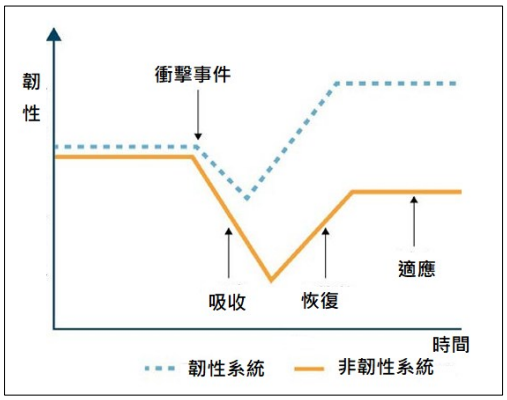
定演練與設施設置，較少從跨災害、跨系統與全生命週期的「防災韌性」角度，系統性評估機場面對複合型與連鎖災害的整體承受、調適與復原能力。相較之下，國際組織如 ICAO、CDRI、FAA 及歐盟等機構，已逐步由傳統災害管理模式，轉向整合風險、韌性導向為核心的機場防災韌性架構，發展出具體評估工具、成熟度模型與制度化推動機制。此一趨勢凸顯我國在機場防災韌性制度、評估機制與跨部門協作，仍存在顯著落差。

因此，本研究係從「機場防災韌性機制」角度出發，蒐整國際在機場防災韌性相關指導文件與文獻、國際組織建議提升機場防災韌性作法、機場強化防災韌性國際案例，檢視我國機場現行防災韌性相關政策與機制在面對新型態、高不確定性災害風險下，透過國際經驗對照，提出具體且可操作之精進課題與政策建議，以做為我國民航主管機關與桃園機場公司擬訂機場政策、策略與進行未來投資規劃參考運用。

二、文獻回顧

(一)機場韌性定義

依據聯合國減少災害風險辦公室(United Nations Office for Disaster Risk Reduction, UNDRR)與環境科學協會(Environmental Science Associates, ESA)對韌性之定義〔5,6〕，韌性指的是一個暴露於危害中的系統、社區或社會，能夠在及時且有效的方式下，對危害的影響進行抵抗(Resist)、吸收(Absorb)、調適(Accommodate)、適應(Adapt to)、轉化(Transform)並恢復(Recover) (如圖 1)，其中亦包括透過風險管理來維持與復原其基本且關鍵的結構與功能。



資料來源：〔6〕。

圖 1 韌性系統與非韌性系統比較

ESA 認為需透過辨識威脅與災害，並進行必要調整，引入或強化未來防護作為與降低風險措施以建立韌性，並將韌性分為以下 3 個階段[6]:

- **事前**(Before)：透過預先的預防與減緩規劃加以抵抗衝擊。
- **事中**(During)：透過事先制定的應變計畫來吸收衝擊。
- **事後**(After)：透過預先規劃的復原策略進行調適。

ESA 歸納當前與韌性相關的議題，通常以實體基礎設施為主要關注對象，然而事實上更高度仰賴營運與規劃流程。機場內部可能存在規劃與管理流程或人力資源方面的問題，導致防災設施無法及時且具成本效益的建置或維護。因此 ESA 建議在整體規劃過程中，應持續將上述 3 個階段與下列 4 項構面(Dimensions)[6]做為核心考量。

- **技術構面**(Technological)：相互連結之實體系統能夠發揮可接受或期望效能的能力。
- **組織構面**(Organizational)：透過組織文化(涵蓋能力、規劃、訓練、領導、經驗與資訊管理等)有效能及有效率管理實體系統之能力。
- **社會構面**(Social)：降低內、外部人力資源與地方社區脆弱度的能力。
- **經濟構面**(Economic)：啟動、加速或暫停與緊急管理及災後復原相關流程的能力。

而機場韌性(Airport Resilience)的定義，綜合國際民用航空組織(International Civil Aviation Organization, ICAO)、ACI、歐洲空中航行安全組織(Eurocontrol)、歐盟官方氣候調適平台(The European Climate Adaptation Platform, Climate-ADAPT)等文獻[7~10]，是指機場及其相關系統在面對各類衝擊與干擾(自然災害、氣候變遷、技術故障、疫情、人為或其他突發事件)時，能夠維持其核心功能、迅速恢復關鍵功能運作，並具備適應和持續改進能力的綜合能力。不僅包括基礎硬體設施的抗損壞能力，也涵蓋營運、治理、災害管理及社會經濟等多層面。

(二)機場韌性主要面向

經蒐整 ICAO、CDRI、ACI 等國際文件，機場韌性主要包含以下 6 大面向[7~15]。

1. 基礎設施韌性 (Infrastructure Resilience)

(1) **定義**：係指確保機場關鍵基礎構件，如跑道、滑行道、航廈、電力、給排水、導航/燈光、通訊等，在面對災害或事故衝擊時，能抵抗、吸收、適應及恢復機場基本運作的能力〔6,7,12〕。

(2) **主要內容**：抗震與耐荷設計、排洪與排水容量、被動與主動防洪設施、跑道道面強化、冗餘電力(發電機、不間斷電源)、耐高溫/高濕材料及自然基礎設施(濕地、海堤)等。

(3) **典型措施**：基礎設施脆弱度評估(Vulnerability Assessment)、關鍵設施分散與備援、定期耐久度檢測與維護等。

2. 營運韌性(Operational Resilience)

(1) **定義**：確保機場在發生干擾(天候、事故、系統故障)時，機場運作流程、航班服務、行李處理及旅客服務等仍能維持關鍵運作功能，並能快速適應及有效恢復之能力〔6,8,12〕。

(2) **主要內容**：替代跑道/滑行道配置、臨時旅客動線與航廈安排、行李系統(BHS)應變、地勤與航務調度備援、供應鏈斷裂應對、臨時運輸接駁與疏運策略。

(3) **典型措施**：營運應變計畫 (Business Continuity / Contingency Plans)、情境演練、彈性班表與替代作業手冊與航空公司/地面服務之標準作業流程協定。

3. 治理與管理韌性 (Governance & Management Resilience)

(1) **定義**：機場單位在面對突發事件、長期壓力或系統性風險時，透過有效的治理架構、決策流程、組織協作與資源管理，確保機場能持續維持策略方向正常運作的能力〔6,12〕。

(2) **主要內容**：緊急應變中心(EOC)運作、指揮鏈(Command & Control)、跨機構溝通機制、風險管理與資源調配、法規及政策層面的協調、情資分享(Information Sharing)機制。

(3) **典型措施**：機場緊急應變計畫(AEP)、跨機構指揮與協調協議(MOUs)、危機決策流程(決策樹)、事後檢討與改進機制。

4. 數位與網路韌性(ICT & Cyber Resilience)

(1) **定義**：機場的資訊系統(ICT)與網路資安系統，在面對資安攻擊、系

統故障、資料外洩、IT 中斷、科技威脅與複雜網路攻擊時，能夠確保資訊系統、航務系統、行李與登機系統、航管通訊等仍能維持關鍵功能或快速回復，並防止敏感資料與控制系統被破壞〔12,13〕。

(2) **主要內容**：關鍵系統備援(異地備援資料中心)、系統可容忍的最長中斷時間/可接受的最大資料遺失量(RTO/RPO)、資安防護(入侵偵測、弱點掃描)、全球衛星導航系統/全球定位系統(GNSS/GPS) 抗干擾措施、供應商/第三方風險管理。

(3) **典型措施**：系統分段冗餘、定期滲透測試、備援通訊路徑、離線手動作業流程、供應鏈系統安全評估、GNSS 監測與替代定位方案。

5. 防災韌性(Disaster Resilience)

(1) **定義**：機場在面對各類突發事件(如自然災害、重大中斷或故障、人為危害、流行病)時，透過有效的準備、預防、應變、協調、持續運作與迅速復原機制，維持關鍵服務不中斷，並確保旅客、機組員與員工安全的綜合能力。涵蓋災前準備、災害應變與災後復原等行動，以降低災害影響，並將其對人民、環境與經濟的衝擊降至最低〔4,6,12,14〕。

(2) **主要內容**：風險與脆弱度評估(Hazard & Vulnerability Analysis)、災害情境模擬、機場緊急應變計畫(Airport Emergency Plan, AEP)、物資與醫療救援準備、災後復原優先順序(Critical Services First)。

(3) **典型措施**：災防演練、災害預警整合、災害後復原排程(Recovery Roadmap)，以及與地方政府/救援單位的協同機制。

6. 環境與氣候韌性(Environmental & Climate Resilience)

(1) **定義**：機場在面對氣候變遷與各類環境衝擊(如極端天氣事件、海平面上升、長期溫度變化、降雨型態改變、水資源壓力及生態影響)時，透過風險辨識、調適規劃、永續設計與營運管理機制，提升機場設施與營運系統對中長期環境變化之適應與承受能力，確保關鍵功能之穩定運作，並在兼顧環境保護與資源效率下，降低氣候與環境風險對安全、營運與經濟所造成之衝擊。

(2) **主要內容**：氣候風險與暴露度評估(Climate Risk & Exposure Assessment)、極端氣候事件對機場設施與營運之衝擊分析(如高溫、強降雨、洪水、乾旱、強風)、海平面上升與沿海淹水風險評估(適用

於沿海或低窪機場)、能源、水資源與土地使用之韌性管理、生態保育與環境品質管理(如噪音與空氣品質)，以及氣候調適與減緩策略(Adaptation & Mitigation)之整合。

(3) **典型措施**：強化排水與滯洪設施、提升跑道與航廈之耐候與耐熱設計、導入再生能源與微電網(Microgrid)以提升能源供應穩定性、建置節水與雨水回收系統、將氣候風險納入機場整體規劃(Airport Master Plan)與設計標準、推動溫室氣體盤查與減量措施，以及建立因應長期氣候變化之調適行動計畫。

7.機場主要韌性面向彼此關聯性

上述 6 大機場韌性主要面向具有高度關聯性，共同形成機場整體韌性的系統化架構(如圖 2)。「基礎設施韌性面向」是實體設施與關鍵系統的承載基礎；「營運韌性面向」如同持續運作的引擎，確保營運與服務不中斷;「治理與管理韌性面向」如同統籌協調與決策制定之中樞核心;「數位與網路韌性面向」如同支撐資訊流通與決策支援的神經系統;「防災韌性面向」則著重在衝擊事件下的整合應變與迅速復原能力；「環境與氣候韌性面向」則是因應氣候變遷與長期環境壓力之調適與承受能力。

圖 2 機場整體韌性的系統化架構

(三)機場防災韌性面向重要性

在機場韌性六大面向中，「防災韌性面向」是機場全面韌性策略最

關鍵的一環，在各類威脅及突發事件中，防災韌性相較於其他機場韌性面向，是最直接影響機場基本生存、運作持續性、快速恢復及跨面向整合的優先領域，具有國家關鍵基礎設施韌性支撐節點的功能，也是提升機場整體韌性不可或缺的核心橋樑。

在實際應用上，「基礎設施韌性面向」的抗災結構設計、「營運韌性面向」的防災計畫應急程序、「治理與管理韌性面向」的協調機制、「數位與網路韌性面向」的通訊保障及「環境與氣候韌性面向」的長期風險規劃，都以「防災韌性面向」為機場韌性的整合實踐。相關研究與實證也顯示，缺乏有效的防災韌性規劃與機制，將大幅降低其他韌性面向的實際效能。

本研究聚焦於「防災韌性面向」，災前透過環境與氣候風險評估調整設計與規劃，降低未來災害衝擊的潛在風險；當災害或重大中斷時，由「防災韌性面向」啟動整合應變機制，「基礎設施韌性面向」負責吸收與承受衝擊，「營運韌性面向」執行降級或替代運作方案，「數位與網路韌性面向」則支撐指揮與通訊；災後由「治理與管理韌性面向」主導復原、改善與投資重整，「環境與氣候韌性面向」進行中長期調適，提升機場對氣候與環境變化的承受能力，並降低未來災害的累積與擴大影響，其他面向則回饋經驗與調整建議至防災韌性面向，進而形成持續精進之機場韌性升級循環。

(四)機場防災韌性相關文獻

1. 機場災害類型

機場災害型態已由過往單一事件，逐漸演變為跨系統、跨面向的複合型災害，對機場基礎設施、飛航安全及營運持續性均可能造成重大影響。隨著全球氣候變遷、航空運輸規模擴張以及機場營運高度數位化，機場所面臨之風險來源亦日益多元且複雜。依相關研究〔11,16,17〕，機場災害可概略區分為以下類型。

(1) **自然災害(Natural Hazards)**

此類型災害主要源於自然環境與氣候條件變化，對機場基礎設施完整性、飛航作業安全及航班運作穩定性具有直接且顯著之影響，並因地理位置與氣候條件不同而呈現高度區域差異。近年在氣候變

遷影響下，極端氣候事件發生頻率與強度均有上升趨勢，已成為影響機場營運韌性的重要風險來源。

A. 極端氣候與氣象事件：包含強降雨、洪水、內澇、颱風、暴風雪、強風、高溫熱浪、寒害、結冰及低能見度(如濃霧、沙塵暴及霾害)等，可能導致跑道或滑行道關閉、航班延誤或取消，以及地面作業受限。

B. 地質災害：如海嘯、土石流、地層下陷及火山灰等，其中火山灰可能影響航空器引擎安全及航路、空域運作，進而造成航班大規模調整或停航。

(2) **人為災害(Man-made / Technological Hazards)**

此類災害主要與機場設施設備運作、工程設計、系統管理及人為操作行為相關，雖具有一定程度之可預防性，但一旦發生，可能對機場營運與飛航安全造成重大衝擊。

A. 航空事故：包括起降事故(如衝出跑道、硬著陸)、航空器與車輛或設施之地面碰撞，以及機坪作業事故等，可能導致人員傷亡、航空器損毀及機場營運中斷。

B. 基礎設施與設備故障：如跑道或滑行道結構損壞、航管與導航助航設備故障，以及航廈電力、空調或行李處理系統失效等，均可能影響航班調度效率與旅客服務品質；另如油料供應、供水或消防系統中斷，亦可能影響機場安全運作。

C. 危險物品與工業事故：如燃油外洩、化學品洩漏、火災或爆炸等事件，除可能造成人員傷亡與環境污染外，亦可能迫使機場部分區域或整體營運暫停。

(3) **數位與網路系統災害(ICT & Cyber Hazards)**

隨著機場智慧化與數位化程度持續提升，資訊與通訊系統已成為支撐機場營運之重要關鍵基礎設施。一旦相關系統受到資安攻擊或技術故障影響，可能迅速衝擊航班資訊發布、旅客服務、行李處理及整體營運調度能力。此類型屬於近年對機場營運衝擊快速上升之高風險類型。

A. 資安攻擊：包括勒索病毒(Ransomware)、系統入侵、資料外洩及分散式阻斷服務(DDoS)攻擊等，可能導致系統癱瘓或營運資料

遭破壞。

B. 資訊系統中斷：如航班資訊顯示系統(FIDS)故障、行李處理系統(BHS)異常、航管或機場營運資料庫(AODB)停擺，以及全球性 IT 供應鏈故障等，均可能造成航班資訊混亂與旅客滯留。

(4) **公共安全與蓄意攻擊事件(Security-related Hazards)**

此類事件多屬蓄意或突發之公共安全威脅，可能對旅客、機場員工及設施設備造成直接危害，並對機場運作秩序及社會安全造成重大影響。

A. 恐怖攻擊：如爆炸、槍擊、自殺攻擊或無人機入侵等，可能造成重大人員傷亡及機場營運中斷。

B. 重大治安或社會事件：如暴動、示威占領、非法入侵或大量人潮踩踏等，可能影響航廈秩序、旅客安全及航班運作。

(5) **公共衛生與生物性災害(Public Health Hazards)**

機場做為國際人員流動的重要節點，亦可能成為疾病跨境傳播的重要管道。重大公共衛生事件除影響旅客健康安全外，亦可能導致邊境管制、航班減班或停飛，並對航空運輸需求及機場營運模式造成顯著影響。

A. 傳染病疫情：如全球或區域性傳染病爆發，可能造成航班運量下降及機場營運模式調整。

B. 生物污染事件：如生物性病原體污染或散播事件，可能影響機場人員與旅客健康，並需啟動緊急公共衛生應變機制。

(6) **複合型與連鎖災害(Compound & Cascading Disasters)**

複合型與連鎖災害係指不同類型災害在時間或空間上相互交互影響，進而引發跨系統、跨設施或跨營運層面的連鎖效應。相較於單一災害事件，此類災害往往將放大衝擊範圍，並使機場營運中斷時間延長、復原難度提高，因此已成為當前機場防災韌性與營運持續管理研究的重要核心議題，例如以下狀況。

A. 極端降雨可能引發機場區域淹水，進而造成電力系統中斷，並進一步影響資訊科技(IT)系統之正常運作。

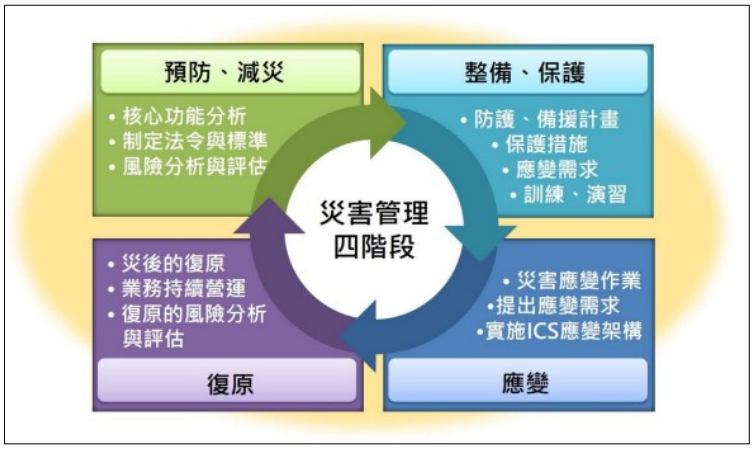
B. 地震可能導致機場基礎設施受損，並進一步造成航管系統中斷，最終引發大規模航班取消或航班運作受阻。

C. 資安攻擊可能造成機場營運系統癱瘓，進而影響機場整體營運功能，並增加公共安全風險。

因此，機場在規劃防災韌性策略時，除需考量單一災害事件外，亦應納入複合型與連鎖災害情境之風險評估與應變機制，以提升整體機場防災韌性與災害應變能力。

2. 機場防災管理循環階段

傳統的防災管理通常分為預防與減災、 整備與保護、應變、復原等四階段循環，詳如圖 3 所示。



資料來源：〔18〕。

圖 3 防災管理四階段循環圖

然而，隨著災害型態日益複雜，災害衝擊已跨系統且具高度不確定性，現今防災思維已逐步由「事件導向」轉向「韌性導向(Resilience-based Disaster Management)」，強調系統在災前、災中與災後的整體承受、調整與演化能力。因此，現代災害管理已不再僅追求「災後復原」，而是透過吸收、調適與轉型等韌性能力的建立〔19〕，使系統能在不確定與複合災害環境下持續運作並不斷進化，爰災害管理可細分並擴展為以下 6 個相互連續且循環的階段。

(1) 減災(Mitigation)：降低災害發生機率與衝擊。

(2) 準備(Preparedness)：建立應變程序、演練、資訊通報。

(3) 吸收(Absorption)：事件發生時維持關鍵功能不中斷。

(4) 調適(Adaptation)：即時調整營運流程、資源、協作方式。

(5) 復原(Recovery)：迅速恢復到可接受的服務水平。

(6) 轉型(Transformation)：從災後經驗改善防災能力。

3. 提升防災韌性核心要件

(1) 風險辨識與脆弱度評估(Risk Identification & Vulnerability Assessment)：辨識暴露的自然災害、人為危害、基礎設施弱點與關聯風險，了解機場可能遭遇的威脅，例如極端氣候、地震、系統故障等。

(2) 預防與減緩策略(Mitigation & Preparedness)：透過工程設計、備援系統、災害模擬演練減少災害衝擊。

(3) 應變與危機管理(Emergency Response & Crisis Management)：明確的機場緊急應變計畫(AEP)、通報鏈、指揮系統(ICS/EOC)、跨單位協作機制與演練。

(4) 適應與學習能力(Adaptability)：面對新型風險能調整策略與措施。

(5) 快速恢復與重建(Recovery)：在災害後迅速恢復完整運作，資金與保險安排，建立長期重建計畫與韌性提升計畫。

4. 機場防災韌性評估方法與指標

(1) 常見評估流程：包含風險與災害識別、韌性構面與指標建構、專家問卷蒐集、因果關係與權重分析，以及績效評估與排序。其中，DEMATEL 法常用於分析各指標間的因果關係與影響程度，VIKOR 法或 TOPSIS 法則用於比較不同機場或不同構面韌性表現，進而辨識優先改善項目。

(2) 訂定量化指標：近期研究多為整合性績效模型以量化韌性，常用指標包含：緊急救災與疏散程序效率、災後復原時間(Time To Recovery, TTR)、關鍵設施快速修復能力、事後檢討與改善機制等。

(3) 建立模型與進行模擬分析：機場防災韌性涉及多種災害型態與跨系統運作，其評估通常採取整合性與系統性方法。近年相關研究多採用混合式多準則決策分析(Hybrid MCDM)，結合專家判斷與量化分析，以同時考量各韌性構面間之相互依賴關係與整體績效表現。建立模型目的是要找出機場韌性最脆弱的部分與需要優先改善項目；而模擬分析是要了解災害發生時，系統可能受到破壞的程度及復原的時間。

A. 混合多準則決策(Hybrid MCDM)模型：李彥呈〔20〕建構模型，以系統化方式評估機場韌性，以德爾菲法彙整並篩選臺灣 3 座國

際機場之韌性關鍵構面與評估準則，運用修正決策實驗室分析法(DEMATEL)結合 Dombi 加權聚合方法，分析各評估準則間因果關係與權重分布，並以修正式折衷排序評估法(VIKOR)評估不同機場在各準則下韌性與改善優先順序。研究結果顯示「災前準備性」為影響機場整體韌性的最關鍵構面，其中以緊急救災與疏散避難計畫之執行能力、快速搶修與復原機制，以及關鍵設施與系統妥善率為最具影響力的評估準則。該研究建構模型，可用於比較機場韌性表現及辨識韌性不足關鍵環節。

B. 其他如 AHP、ANP、TOPSIS 法等，也適合用於指標加權與機場間韌性比較。

C. 韌性成熟度模型(Maturity Model)可分級呈現(初階→成熟)，適合機場政策監理與追蹤改善。

D. 情境模擬與壓力測試，可驗證機場營運持續計畫(Airport Business Continuity Plan, BCP)與系統備援能力，並評估極端情境下的失效點。

三、國外機場重大災害事件

(一)濟州航空 2216 號班機空難事件

1. 事件分析

(1) **災害概述**：2024 年 12 月 29 日濟州航空(Jeju Air)2216 號班機(機型為波音 737-800)由泰國曼谷飛往南韓務安國際機場(Muan International Airport)，在接近機場時遭遇鳥擊，鳥類碎片吸入引擎，造成推力損失。飛行員發出緊急通報並嘗試復飛，在第二次嘗試降落時，起落架未成功放下，導致飛機以機腹著陸，之後衝出跑道並撞上跑道末端混凝土結構，致機體斷裂並爆炸起火，造成 179 人罹難慘重傷亡(如圖 4 所示)，成為南韓史上最嚴重的民航空難，也是濟州航空成立以來首起致命事故[21]。

資料來源：〔21〕。

圖 4 濟州航空 2216 號班機空難事故現場

(2) **事後檢討**：南韓航空事故調查委員會(ARAIB)於災後指出，鳥擊雖為起因，惟飛行員在引擎發生問題後關閉了正常運作的左引擎，而不是遭鳥擊受損的右引擎，可能才是導致致命空難之原因。事故中飛機亦未能成功部署起落架進行正常降落，直接以機腹著地，加劇飛機失控與衝出跑道的風險，加上飛機衝出跑道後撞上機場跑道末端的混凝土結構，使傷亡情形更加嚴重。

2. 其他機場內空難案例

(1) 2024 年日本航空降落羽田機場時，與海上保安廳 DHC-8 海上巡邏機在跑道相撞事件。

(2) 2025 年美鷹航空降落美國隆納·雷根華盛頓國家機場時，在距離跑道 800 公尺與美國陸航 UH-60 直升機相撞墜入波多馬克河事件。

(二)日本大阪關西機場風災事件〔22〕

1. 事件分析

(1) **災害概述**：2018 年 9 月 4 日颱風燕子(Jebi)帶來強風與風暴潮，關西機場(KIX)所在人工島遭海水倒灌，大部分跑道、滑行道、貨物區域與航廈設施淹水，導致跑道關閉 10 天，航廈關閉 17 天，航空客、貨運及航站電力停擺，且一艘失控油輪撞毀連接本島與機場之聯絡橋(Causeway)，導致陸上交通完全中斷(如圖 5)，數千名旅客與機場人員受困，至 2018 年 10 月才逐步恢復完整運作，經濟損失估約達 5 億美元。

資料來源：〔22〕。

圖 5 日本大阪關西機場 2018 年風災狀況

(2) **事後檢討**：極端氣候及航站構造弱點(人工島、單一出入橋樑)。

2. 其他類似案例

(1) 2011 年泰國曼谷廊曼機場(DMK)大洪災事件。

(2) 2012 年美國紐約拉瓜迪亞機場(LGA)颶風(Sandy)及洪水事件。

(三)布魯塞爾機場恐怖攻擊事件

1. 事件分析

(1) **災害概述**：2016 年 3 月 22 日，比利時布魯塞爾機場(Brussels Airport, BRU)航廈出境大廳發生連環自殺炸彈恐怖攻擊事件，死亡約 35 人、受傷約 340 人，並導致機場隨後數日甚至數週關閉進行重建。事件不僅嚴重衝擊航空運輸系統，也對比利時及歐洲整體公共安全與社會穩定造成重大影響〔23〕。

(2) **事後檢討**：機場人流密集，無法兼顧旅運效率與全面安檢；事前對恐怖攻擊威脅情資整合與風險評估不足，未能有效轉化為具體的預防性安全部署；安全設計以空側為核心，對災前預防與災中即時應變的整合韌性考量不足。

2. 其他類似案例

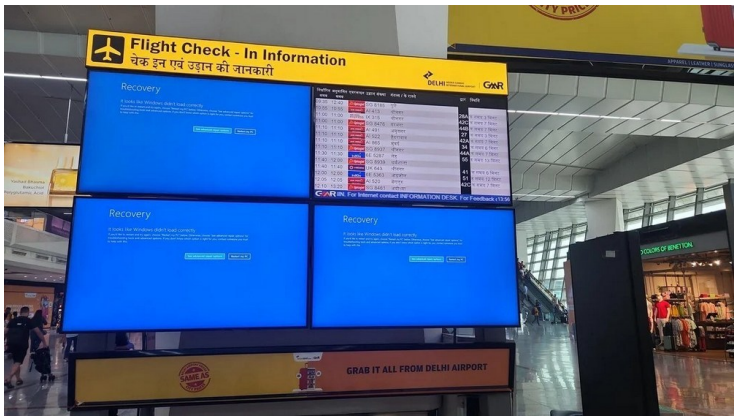
(1) 2011 年莫斯科多莫傑多沃機場(Domodedovo Airport)恐怖攻擊事件。

(2) 2016 年伊斯坦堡阿塔圖克機場(Atatürk Airport)恐怖攻擊事件。

(四)全球機場 IT 系統故障事件

1. 事件分析

(1) **災害概述**：2024 年 7 月由於美國網路安全公司 CrowdStrike 異常更新作業，導致全球大量客戶的 Windows 作業系統電腦和虛擬機器裝置出現故障，顯示為藍白畫面或自動進入系統修復介面[24](如圖 6)，波及多個行業造成眾多服務中斷。微軟初估該故障影響全球近 850 萬台裝置，大型國際機場運作均受嚴重影響，導致報到、行李、航班資訊及地勤作業系統癱瘓，大量航班延誤，共有 5,078 班航班(占定期航班的 4.6%)被取消，專家稱之為「史上最嚴重的 IT 故障事件」。



資料來源：〔24〕。

圖 6 CrowdStrike 資安軟體異常更新導致機場 IT 故障狀況

(2) **事後檢討**

A. 高度依賴單一商用資安產品

多數機場與航空公司廣泛部署相同端點防護軟體，一旦核心供應商發生更新異常，即形成單點失效(Single Point of Failure)風險。

B. IT 系統與營運系統高度耦合

機場關鍵營運流程(報到、行李、航班資訊)與 IT 系統整合度高，缺乏離線或手動備援流程，使 IT 故障迅速演變為全面營運中斷。

C. 更新控管與測試機制不足

自動化更新未經充分分批測試或隔離環境驗證，即直接部署至正式營運系統，導致錯誤更新同步擴散至全球。

D. 跨部門與跨系統應變協調不足

IT、資安、營運與地勤單位在即時應變與決策流程上缺乏預先演

練，延誤故障排除與人工替代作業的啟動時機。

2. 其他類似案例

(1) 2020~2022 年英國航空(British Airways)多次 IT 故障事件。

(2) 2021 年瑞士航空與歐洲多座機場 SITA 系統中斷事件。

(五)歐洲多機場作業系統遭勒索病毒攻擊癱瘓事件

1. 災害分析

(1) **事件概述：**2025 年 9 月 19~20 日，英國倫敦希斯洛機場(Heathrow)、比利時布魯塞爾機場(Brussels)、德國柏林布蘭登堡機場(BER)、愛爾蘭都柏林與科克等歐洲主要機場遭到駭客入侵 MUSE (Multi-User System Environment) 軟體系統(為多家航空公司提供共用報到與登機平台)，以勒索病毒(Ransomware)攻擊，導致機場自動報到、登機與行李系統癱瘓，數百班航班延遲或被取消，迫使地勤人員轉為人工報到與登機作業，造成數千名旅客滯留(如圖 7)。

資料來源：〔25〕。

圖 7 歐洲機場遭勒索病毒攻擊導致旅客滯留情形

(2) **事後檢討**

A. 依賴單一第三方供應商系統

多座國際機場與航空公司共同採用同一通用報到系統平台，攻擊核心服務供應商即造成廣泛效應。

B. 攻擊供應鏈

勒索者利用 IT 供應鏈一體化架構弱點，先滲透至航空供應商系統，再藉由該系統往下波及多座機場。

C. 缺乏足夠隔離與備援系統

多座機場未提前準備足夠隔離的替代平台，導致一旦 MUSE 系統癱瘓，不能迅速以備援系統自動接手，只能靠人工暫時因應。

D. 未充分預期高度數位化服務中斷風險

在高度倚賴數位系統自動報到與行李處理的狀態下，系統不堪中斷而直接影響整體營運，此風險原本未被充分納入嚴重災害風險評估中。

2. 其他類似案例

(1) 2018 年英國布里斯托機場勒索病毒攻擊事件。

(2) 2019 年美國彭薩科拉市勒索病毒攻擊事件。

四、國際組織建議提升機場防災韌性作法

(一)CDRI 建議邁向韌性機場 5 大步驟[4]

CDRI 在 2023 年發布《全球機場防災韌性研究》(The Global Study on Disaster Resilience of Airports, GSDRA)第一階段報告[14]，該報告記錄機場韌性各面向，並 54 個國家中的 111 座機場進行問卷調查與焦點團體討論，了解氣候風險對機場所造成的關鍵影響、災害影響動態、風險評估以及機場的適應能力。研究結果顯示機場導入調適措施與風險減緩策略具有迫切性，可有效因應氣候變遷與環境因素所帶來的風險。而且風險評估的執行頻率、韌性規劃及機場全生命週期之永續實務作為，對於與全球氣候目標接軌具有關鍵意義。

CDRI 建議「邁向韌性機場的 5 大步驟(Five Steps towards Resilience of Airports)」[4,14]，提供各國政府、機場營運單位及其他利害關係機構依循，以系統性理解機場資產所面臨的災害風險，並擘劃強化機場韌性的具體途徑，進而獲得強化機場韌性的效益，步驟內容摘整如下：

步驟 1：定期進行機場脆弱度評估

機場脆弱度評估(Periodic Vulnerability Assessments, PVAs)屬於規模較小且具重複性的評估作業，旨在系統性與持續性識別、分析與排序機場基礎設施(如跑道、航廈、電力系統與通訊系統等)的潛在弱點與風險，評估各類災害發生的可能性及其潛在影響，使機場能夠有效因應脆弱點、有效管理不斷演變的威脅、強化災害應變能力

及提升整體韌性，並進而保障其關鍵資產。

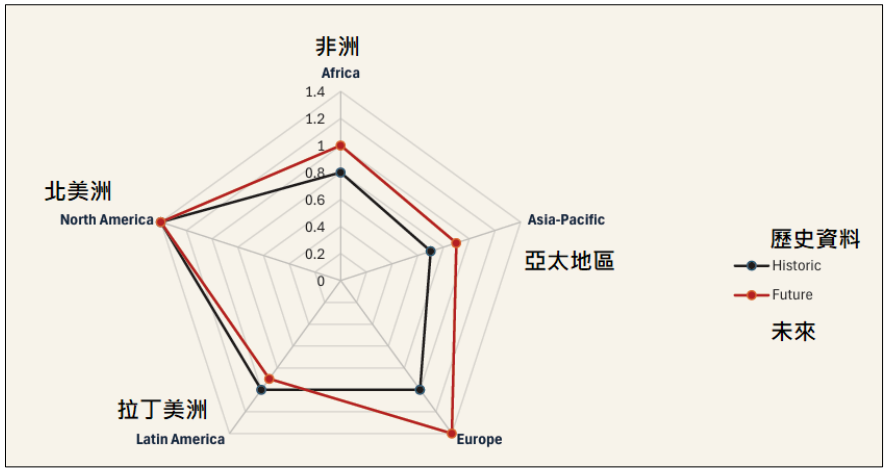
根據 CDRI 在 2023 年的調查結果〔4,14〕，僅 71%受訪機場執行 PVA，其中 55.3%機場每年進行一次評估，27.7%機場每 2~5 年進行一次評估，甚至有 17%機場超過 5 年才進行一次評估。CDRI 建議機場單位應依其地理條件與治理脈絡，定期自行執行此項評估作業，並建議可考量 ICAO 所提出，且為航空產業中廣泛採用的風險評估矩陣與評估架構，做為執行定期 PVA 的重要參考基準。

步驟 2：將脆弱度評估擴展為全面性的風險與韌性評估

全面性的風險與韌性評估，係指系統性且全面性檢視機場在面對各類干擾事件發生前、發生期間及發生後，承受衝擊並從中復原之能力。此類評估不僅納入先前所完成的各項定期 PVA，並進一步涵蓋機場營運所有層面，包括實體基礎設施、組織架構以及緊急應變程序等。評估目標在於識別並排序潛在威脅、評估脆弱性，並擬訂風險緩解策略，以提升整體韌性。

需進行全面性評估的原因是，各類災害如風暴、強降雨、洪水、極端高溫與結冰、乾旱及火山活動，在影響的複雜度與性質上不盡相同。若未能充分理解這些潛在衝擊，將可能削弱機場於災後的營運表現，並造成嚴重的經濟與財務障礙，因此進行全面性評估有其必要性，可確保韌性規劃的完整性，並強化機場設施面對各類潛在災害的整體整備能力。然而，CDRI 調查結果顯示，71%受訪機場僅進行 PVA，尚未進行全面性的風險與韌性評估。

CDRI 建議此項評估主導角色應是機場經營單位，可借助國際研究機構的專業支援，並由相關政府部門提供必要資料及發布評估指引，以利在國家層級推動評估作業的標準化，使各機場評估結果具備可比較性。CDRI 建議評估指標應涵蓋兩項關鍵基準，第一是「恢復營運(重新啟動作業)所需的時間」；第二是「全面復原並恢復機場正常功能所需的時間」。另外，CDRI 以災害嚴重度評等系統評估全球機場某類災害的嚴重度分布情形如圖 8，將災害嚴重程度劃分為 0 至 5 級，5 級代表最高嚴重度。該整體評估結果顯示，所有受調查機場中，極端風暴的嚴重程度最高，其次為極端降雨。



資料來源：〔4〕。

圖 8 各地區機場災害衝擊的平均嚴重程度雷達圖

步驟 3：建立對機場風險承受度的廣泛認識

風險承受度(Risk Appetite)係指機場在面對天然災害時，所願意接受的風險暴露程度，界定了該機場組織運作的風險邊界，並形塑策略方向與決策流程。風險承受度越高，代表該機場願意容忍較大的干擾風險，以換取潛在效益；反之，較低的風險承受度則意味著犧牲彈性或成本效率，即有降低營運中斷發生的可能性。確認風險承受度可進行前瞻性的風險管理，在不確定情境下做出更具資訊基礎決策，並優化因應作為，對於保障資產、降低營運中斷風險，並確保長期韌性具有關鍵作用。

CDRI 建議機場經營單位應在產業專家的協助下，進行相關研究以理解並界定自身的風險承受度，政府部門可提供必要資料，並發布方法指引，以在國家層級推動此類評估的標準化，使各機場之評估結果具備可比較性。

步驟 4：與利害關係人有效合作，共同提升機場韌性

機場與各級政府機關在調適與整備規劃上具有相互依賴性，因此需要透過有效合作(Effective Collaboration)，促進跨部門、跨組織的合作行動，包括政府機構與監理機關、地方政府、緊急應變單位、社區組織、鄰近機場以及其他相關機構之間的夥伴關係與溝通，全面評估整體風險，並確立共同承擔責任的治理架構與權責範圍，包括應變計畫協調、資源共享、辦理聯合演練，以及整合行動方向，確

保在可能影響機場營運的潛在危害或緊急事件發生時，能夠形成一致、有效、正式與長期的整體應變機制，並共同規劃、整備並落實各項策略，俾提升機場面對災害時的整體韌性。

步驟 5：建立統一制度促進合作與分享，建立整合防災韌性計畫

多數機場雖已制定個別緊急應變計畫，並載明災害發生時的處置流程，但多數未充分涵蓋災害所帶來的財務衝擊；且災害發生時，其影響往往不僅限於機場，而是波及整個區域，因此整合納入各類利害關係人進行整合防災韌性計畫(Integrated Disaster Resilience Plan)至關重要，尤其是與機場具有相互依賴關係的關鍵基礎設施單位，如電力與自來水公司等。

整合防災韌性計畫係由組織、社區及其他相關利害關係人共同制定的整體性策略，目的在於因應災害的事前整備、即時應變、災後復原以及衝擊減緩。此類整合式計畫將災害管理的不同面向納入一致且協調的架構中，整合跨部門與跨利害關係人的行動與資源。可確保在緊急事件發生時，具備更強韌、更協調且更有效的應變能力，不僅保護機場本身，也同時守護周邊社區。CDRI 建議由機場主管機關建立此整合性制度架構，使機場單位能夠與所有相關利害關係人共同制定整合防災韌性計畫。

(二)FAA 推動韌性管理計畫[6]

(1) **推動緣由:**美國聯邦航空總署(FAA)有感於傳統韌性規劃多半聚焦於關鍵營運基礎設施，且著重於突發性衝擊事件(Shock Events)發生後的應變，而忽略不可或缺的關鍵要素-慢性壓力源(Chronic Stressors)如容量限制、延後維護、基礎設施老化、經濟衰退/景氣下滑、氣候變遷衝擊、社會經濟脆弱性及反覆發生、頻率更高且影響更嚴重的事件型態等，因此認為有必要及早發展及落實韌性管理計畫(Resilience Management Plan, RMP)，辨識威脅與災害風險，以降低或預防突發性衝擊事件與慢性壓力源相關的風險。

(2) **計畫內容:**韌性管理計畫是一種加強版的營運連續性規劃(Continuity of Operations Planning, COOP)，以系統化、前瞻性、風險評估為基礎，對機場所有業務面向資產與基礎設施進行持續動態營運管理，協助

機場辨識並對關鍵資產系統與基礎設施進行優先排序，以提升機場單位因應突發性衝擊事件與處理慢性壓力源的能力，確保基礎設施、營運關鍵實體系統與人力系統完整連結。關鍵資產不限於實體設施(如跑道與航廈)，也包括人員(如機場與營運單位員工)及流程(如資本規劃與設施/資產管理計畫)。韌性管理計畫也與既有管理系統互補，可促進與其他相關系統間資訊交流與協調，確保所有風險皆能被充分理解與管理。

(3) **韌性管理計畫規劃核心要素**

- 策略與願景構建
- 分析與評估
- 規劃與文件化
- 系統建置
- 檢討與更新的流程

(4) **韌性管理計畫規劃概念流程**

A. 建立專案架構
B. 願景構建
C. 策略性資產與基礎設施盤點
D. 需求確認
E. 風險評估
F. 辨識策略重點領域
G. 發展聚焦式管理計畫與流程
H. 利害關係人參與
I. 建立韌性管理系統
J. 發展韌性推廣與教育計畫
K. 建置電子化韌性管理工具
L. 建立定期檢討與審查機制

五、機場強化防災韌性國際案例

(一)荷蘭

1. 建立全面整合的國家級防災韌性治理模式

(1) **實施內容：**將全國劃分為 25 個安全區域(Security Regions)，採行一套全面且整合的防災韌性治理模式，每一安全區域均負責保障其轄區內居民與訪客的安全，並協調多項領域的工作，包括消防服務、

醫療救助、公共秩序與安全，以及災害與危機管理。整合模式的關鍵在於明確界定各安全區域所肩負之預防與撲滅火災責任，並確保具備完善設備與受過訓練的人力資源。各安全區域亦須透過制定特定風險概況(Risk Profiles)與量身打造的管理策略，強化風險整備與災害應對能力〔4〕。

(2) **推動成果**：此一制度架構促進了荷蘭建置防災合作與知識分享的整合性機制，最終形塑出一套一致且具高度之防災韌性的國家級策略。

2. 阿姆斯特丹史基浦機場建立風險偏好

(1) **實施內容**：史基浦國際機場(Schiphol International Airport)是荷蘭的重要樞紐機場，位於填海造地且低於海平面場域，長期面臨淹水風險。為降低對降雨型洪水(Pluvial Flooding)的脆弱度，該機場於 2017 年進行一項詳細的降雨型洪水壓力測試，並結合機場空側專家的專業意見進行洪水影響更新評估，詳細分析降雨型洪水對機場造成影響的發生機率、嚴重程度及相關的直接與間接成本〔4〕。

(2) **推動成果**：該機場建立了「風險偏好」(Risk Appetite)，明確界定對極端降雨事件的最適容忍水準，並進一步擬定嚴格的規範要求。雖然實施該改善措施必須投入可觀資本，但降低潛在損害與營運中斷風險所產生的效益已可抵銷並支撐資本投入。

(二)亞特蘭大機場-打造高度韌性的 IT 基礎設施〔26〕

1. **實施內容**：亞特蘭大機場是全球最繁忙機場之一，年旅客逾 1 億人次，對韌性要求極高，2024 年初與 TSA 合作進行風險評估，其 IT 韌性建設的核心目標是：「即使在重大中斷事件下，關鍵航班與旅客服務不中斷或必須快速恢復。」該機場實施以下措施：

   (1)建立 IT 全面不中斷設計(High Availability)

   A. 建立多層級 IT 備援架構。

   B. 核心系統(航班資訊、行李系統、安檢、航管支援)不再依賴單一資料中心，具備即時或近即時切換能力。

   (2) 建立雙資料中心(本地資料中心、異地備援資料中心)備援及雲端服務混合架構，預計 2026 年完成，預算 6,000~8,000 萬美元。

   (3) 深度整合 IT 系統與電力系統，IT 機房列為最高等級關鍵設施。

(4) 建立 24/7 網路營運中心(NOC)，建設 1.4 億美元全機場光纖環網(覆蓋全機場 3.3 萬英畝)與資安監控。

(5) IT 韌性設計直接支援航班資訊顯示系統(FIDS)、行李處理系統(BHS)、航空公司與 TSA 作業系統。

(6) 強化資安工具與服務，修補管理軟體(McAfee ePolicy Orchestrator)、以 MSSP 持續監控 IT 與網路基礎設施，以暗網偵測工具監控潛在資料外洩。

(7) 實施實戰復原演練與網路控制性中斷測試，確保交換機失效時備援自動切換，提升整體業務持續性，並建立員工應對突發狀況的信心。

2. **推動成果**：亞特蘭大機場透過高可用性 IT 架構、雙資料中心與雲端整合、電力與資通訊跨系統備援設計，單一系統或設備故障不再造成全機場營運癱瘓，在極端事件(停電、火災、網路中斷)下恢復時間大幅縮短，即使區域性或城市層級停電，機場 IT 核心系統仍可長時間持續運作，IT 不再是單點失效(Single Point of Failure)。IT 韌性呈現累積式提升，加上持續性的事件後學習機制，成功將 IT 系統由營運風險來源轉化為營運韌性核心支柱。

六、我國機場防災韌性相關政策與機制

(一)機場定位與管理機制

1. 國家關鍵基礎設施

美國遭受 911 恐怖攻擊之後，美國國土安全部(Department of Homeland Security, DHS)近年提出關鍵基礎設施防護(Critical Infrastructure Protection, CIP)風險管理的重要概念。行政院國土安全辦公室自 2009 年 12 月起委託產、官、學界進行「行政院國家關鍵基礎設施防護計畫專業服務委外研究」，將我國國家關鍵基礎設施[2]分為 8 個部門，「交通」為其中之一。另根據行政院公告之《國家關鍵基礎設施安全防護指導綱領》〔27〕附件之「國家關鍵基礎設施領域分類」，

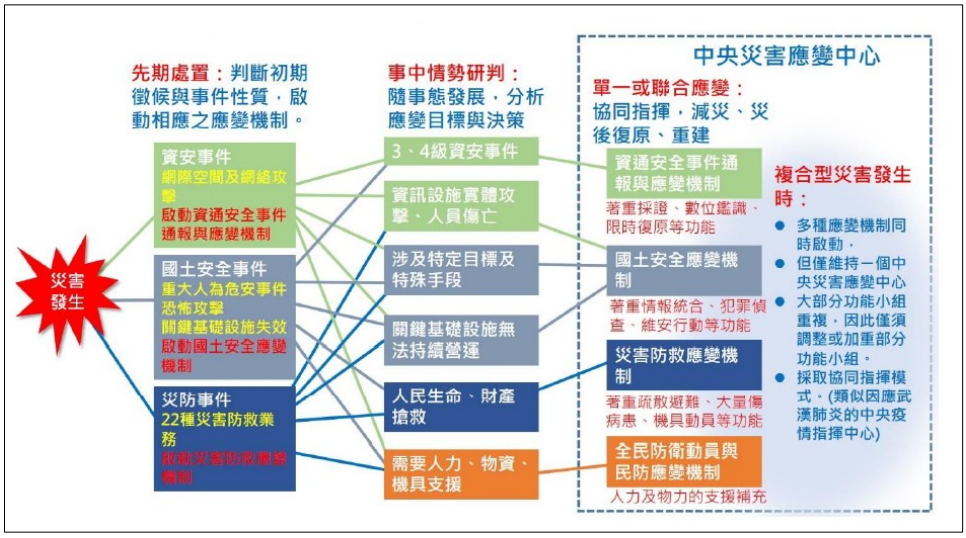
[2] 國家關鍵基礎設施(Critical Infrastructure, CI)，係指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞者。

明列「交通」為主領域之一，「空運」為「交通」之次領域，因此我國機場屬於國家關鍵基礎設施。

國家關鍵基礎設施的防護演習〔28〕是跨機關、單位演習，以全災害觀念結合複合型災害模式實施，與《民防法》、《災害防救法》、《全民防衛動員準備法》、《資通安全管理法》、《國土安全應變機制行動綱要》各整備及應變處置規範息息相關，其應變機制與運作模式如下：

在災害發生時，初步依事件現場狀況判斷，如純屬人員傷亡、設備毀損之災害，則啟動「災害防救應變機制」，優先搶救生命財產，並視狀況請求「全民防衛動員機制」支援；如屬資安事件，則啟動「資通事件通報與應變機制」；後續隨情資及蒐證結果，如判斷涉及特定目標及特殊手段，則啟動「國土安全應變機制」，其運作模式如圖 ；若是複合型災害則是多種應變機制同時啟動，但只維持一個中央災害應變中心，採取協同指揮模式。機場屬於國家關鍵基礎設施，因此遭遇災害事件即是按照該應變機制與運作模式進行防災作業。

另外，《國家關鍵基礎設施防護計畫》也設定國家關鍵基礎設施安全防護目標、說明如何辨識設施資產、系統與網絡，以及如何進行風險評估，從而決定防護優先順序，以實施防護管理計畫，並於事後衡量實施成效。



資料來源：〔28〕。

圖 9 國家關鍵基礎設施災害應變機制與運作模式

2. 機場營運持續計畫

機場屬高複雜、高關聯系統，任一環節中斷，都可能連鎖影響整體航空運作。「機場營運持續計畫」(BCP) 是屬於營運韌性的制度化工具，係指機場在遭遇重大災害、系統故障、資安攻擊或突發事件時，能確保關鍵營運功能不中斷，或於可接受時間內恢復之整體規劃與管理機制。

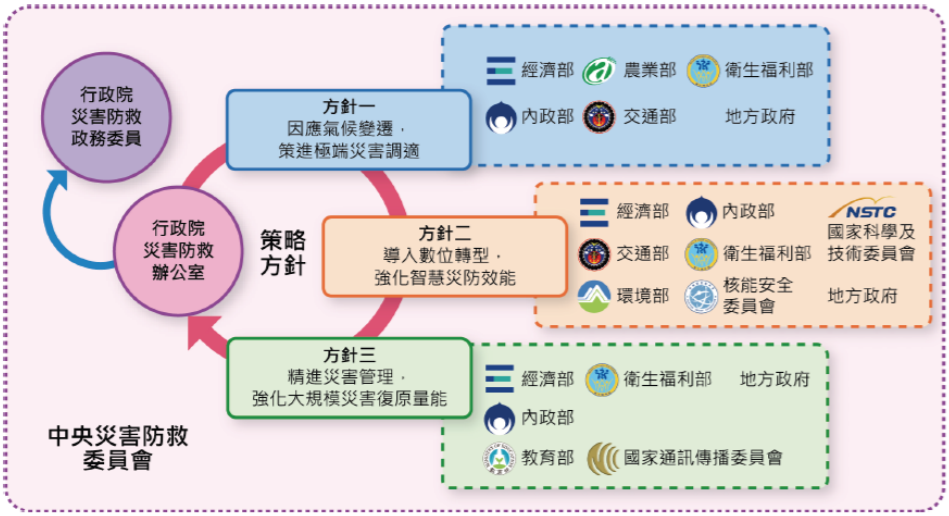
BCP 的核心不是「零事故」，而是「可容忍中斷、可控復原、可持續服務」，也是災後復原工具，更是確保國家關鍵基礎設施在複合災害與資安威脅下，維持最低營運能力的核心制度，其成熟度直接影響機場整體韌性水準。

(二)我國災害防救法制與體系架構

1. 全國整體法制與體系架構

臺灣機場防災韌性建構於《災害防救法》之法制下，整合各級機關資源與操作。法定計畫如《災害防救基本計畫》〔29〕，係由中央災害防救委員會擬訂、中央災害防救會報核定，計畫位階屬綱要性全國災害防救指導計畫。該計畫規範中央政府與地方政府在災害預防、應變與復原重建權責與程序，明定我國災害防救施政之基本方針及策略，擘劃未來 5 年災害防救推動施政藍圖，揭示災害防救方針與策略。

為確保前述基本計畫訂定的基本方針及策略能整體落實推動，行政院建立跨部會之災害防救基本計畫統合推動機制，以專案小組架構推動(如圖 10 所示)，由行政院災害防救政務委員督導運作，行政院災害防救辦公室擔任專案小組的行政幕僚，並由三大方針與 19 項策略主導機關之副首長層級代表負責執行與協調各策略推動。該計畫也明定災害防救計畫體系，各災害防救業務主管機關據以研訂災害防救業務計畫，地方政府機關據以訂定地區災害防救計畫，形成國家防災韌性支撐體系，如圖 11 所示。



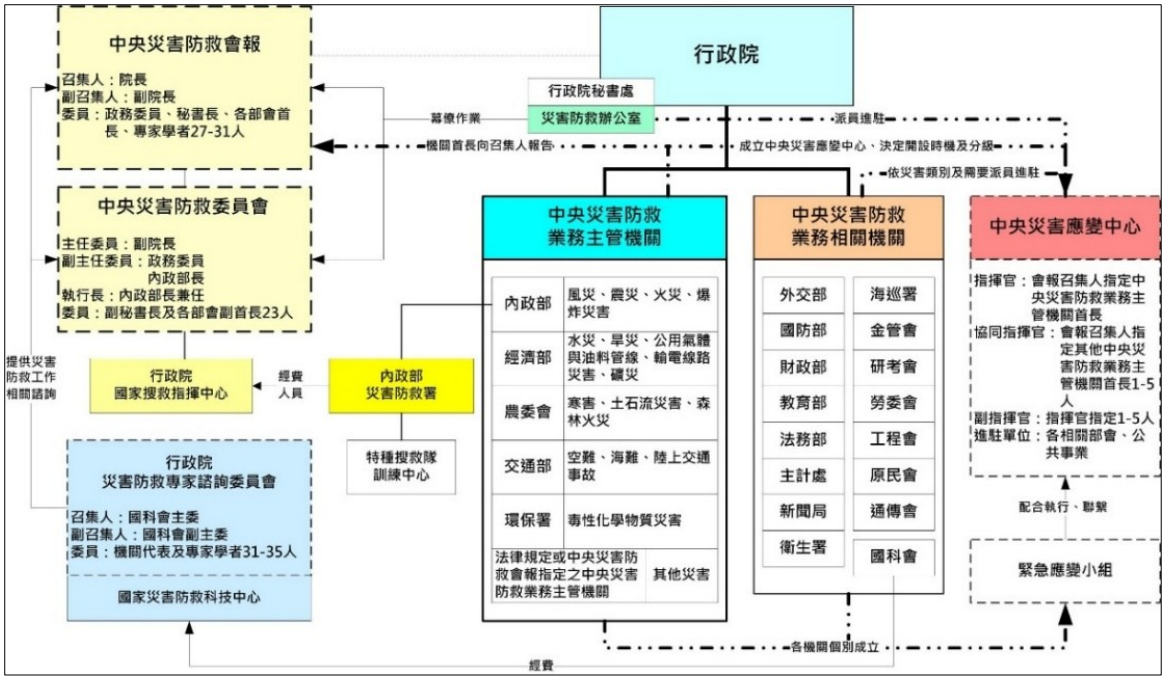
資料來源：〔29〕。

圖 10 災害防救基本計畫統合推動專案小組架構

資料來源：〔29〕。

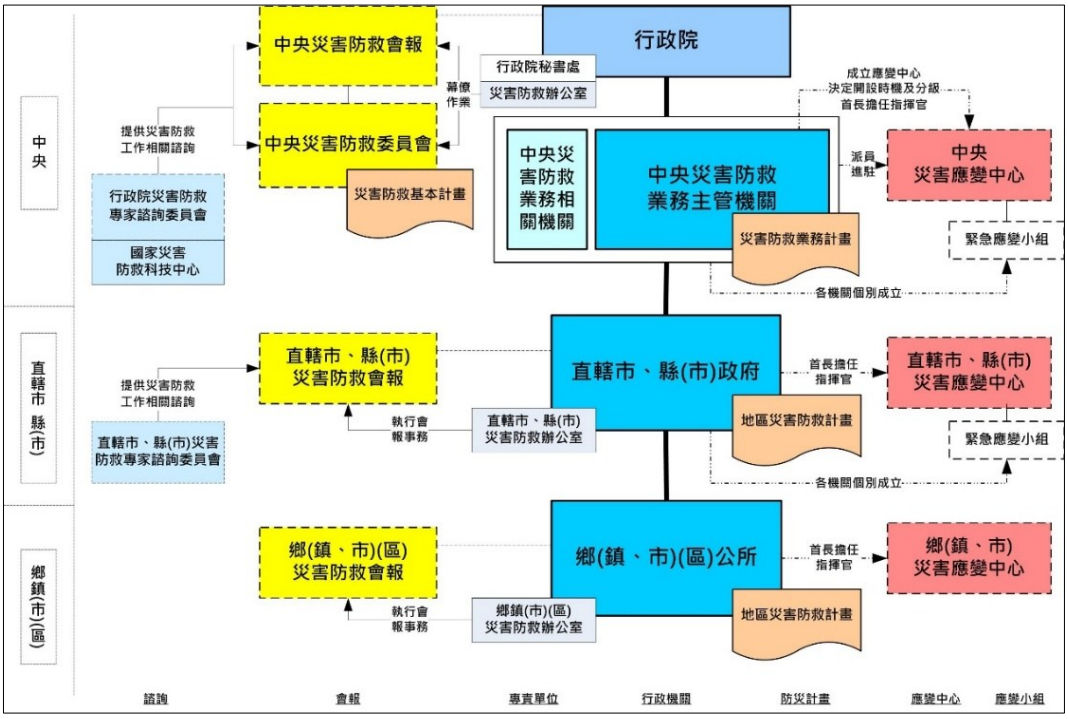
圖 11 災害防救計畫體系

另外，行政院中央災害防救會報官方網站則明確說明中央災害防救體系組織架構及中央、直轄縣市、鄉鎮市等三層級災害防救體系架構〔29〕，以利分層負責災害防救政策、計畫擬訂與執行工作，詳如圖 12、圖 13 所示。



資料來源：〔30〕。

圖 12 中央災害防救體系組織架構



資料來源：〔30〕。

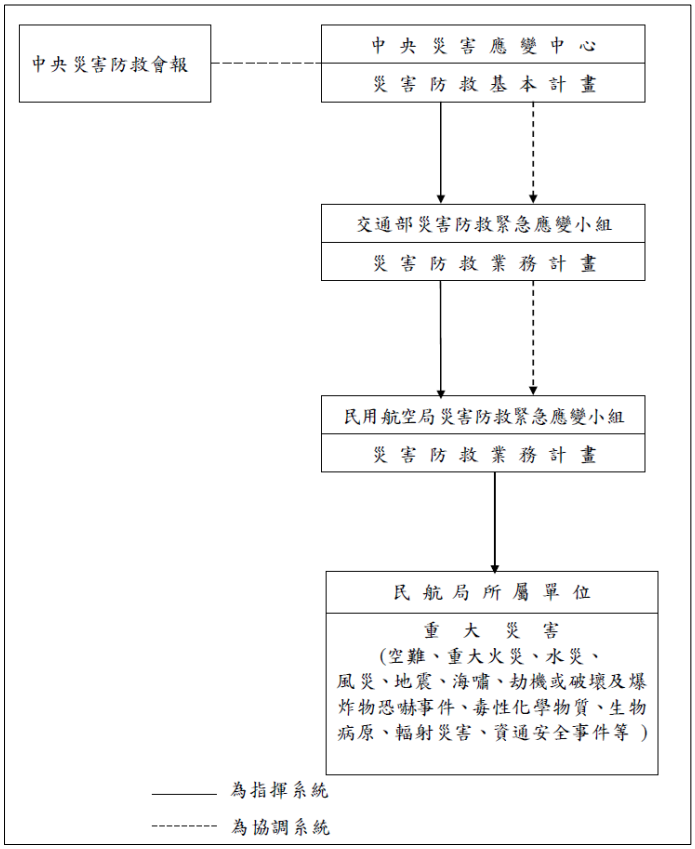
圖 13 中央至地方防救體系架構

《災害防救基本計畫》中，施政基本方針及策略並未逐一列舉每一類關鍵基礎設施細節(包括機場)，但提及需要檢視及評估機場現有設施

之環境脆弱度與防護能力，並強化其於氣候變遷下之耐震與防護計畫。因此機場防災具體執行面，是由《民航局災害防救業務計畫》所明定。

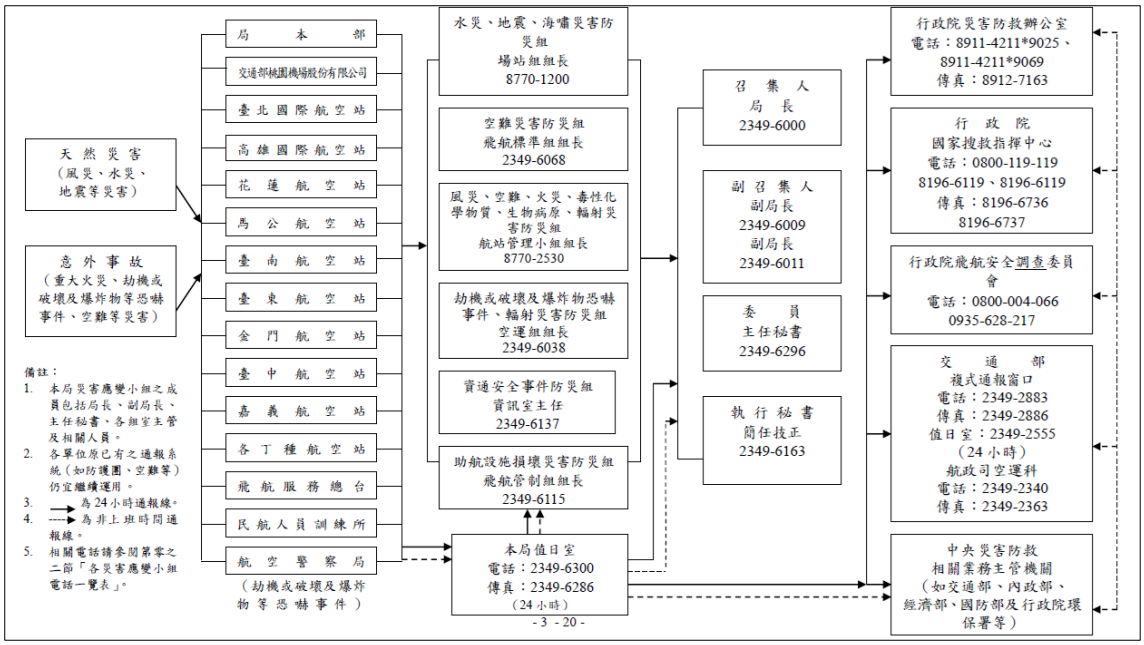
2. 民航局暨所屬航空站災害防救計畫與體系

民航局依據《災害防救法》、《災害防救基本計畫》、《交通部災害緊急通報作業要點》成立「交通部民用航空局災害應變小組」，並訂定《民航局災害防救業務計畫》[31]以動員執行其中各項防救應變措施。該應變小組與中央、交通部及所屬單位之災害防救體系詳如圖 ；民航局、所屬航空站及桃機公司防救災組織架構及重大災害通報程序(如圖)。



資料來源：〔31〕。

圖 14 交通部民航局緊急災害防救體系



資料來源：〔31〕。

圖 15 民航局、航空站及桃機公司防救災組織架構及重大災害通報程序

《民航局災害防救業務計畫》內容涵蓋災害預防、災害應變與善後復原，其中災害預防包含空難災害防救演習，係由各航空站每年辦理一次或配合萬安演習辦理；另外重大火災、地震、水災、劫機或破壞及爆炸物恐嚇事件、毒性化學物質等災害防救演習，每年至少擇一舉辦或觀摩其他單位演習一次。演習及(或)災害發生之後，律定詳加檢討災害防救業務計畫實施過程，並對計畫不適當部分加以修改或重新策訂。

各航空站則制定年度《災害防救業務計畫》，依據《災害防救法》、《災害防救基本計畫》及民航局《災害緊急通報作業要點》設計防災與應變處理程序，包含各災害類別的對應流程與責任分工，以及常態檢視、應急指揮與跨單位協作機制。

(三)交通部暨所屬單位韌性相關政策或規劃

交通部 2020 年版「運輸政策白皮書」空運分冊〔32〕中，與韌性相關的策略為「依機場定位推動機場建設並強化運作韌性」，對應行動方案為「強化機場韌性，推動機場跑滑道、航廈、機電系統等主要設施總體檢機制」，其韌性面向較屬於「基礎設施韌性面向」及「營運韌性面向」。

民航局在 114 年 10 月完成之「臺灣地區民用機場 2045 年系統規劃」[33](尚未奉行政院核定)中，以「東亞最具競爭力之機場群」為願景，並以「多元門戶升級，地方穩健共榮」為目標，將「確保安全韌性」訂為五大發展標的之一(如圖 16)，為最優先事項，也是機場營運首要目標。該標的展開為以下三大策略面向，策略中有關防災韌性要點摘列如下：

資料來源：〔33〕。

圖 16 全國機場系統發展願景、目標及標的

1. **預防能力策略**：即提升硬體設施抗風險之能力，從事前即降低因天災、設施老舊、外力入侵損壞等事件發生之機率。其中「強抗災能力設計」係要求於天災發生時能維持機場正常運作；進行建物設施新建或整建時，應評估設計強抗災能力等級，降低災害對機場造成衝擊之機率。
2. **應變能力策略**：即針對日常業務運作，強化標準作業流程與即時應變機制，以於事件發生後，機場本身能快速對應、恢復致原有狀態。其中「緊急聯絡機制」係於事件發生時即時流通消息，控制各環節作業狀況、調派資源進行協助，運用內、外部資源達到快速復原。
3. **備援機制策略**：即與外部建立即時聯絡與調度支援機制，以於事件發生後結合跨單位能力迅速復原，包括:

(1) **跨運具疏運**：平時應建立空、海、陸運間即時資訊交換機制，以及疏運資源調度方式，以保障我國人民基本運輸需求。

(2) **跨機場備降**：各區域門戶國際機場應具備一定設施等級，確保備降可能性，減少返航、轉降海外帶來的風險與對旅客產生的不便。

(3) **資訊、飛航管制系統及其他設備**：針對營運具有重要影響之資訊系

統及飛航管制系統，採取備援機制(如：雙主機、雙網、雙系統架構或異地備援方案)，或針對其他營運用設備進行緊急維修材料儲備，以確保於突發狀況時，系統與設施仍可穩定運作。

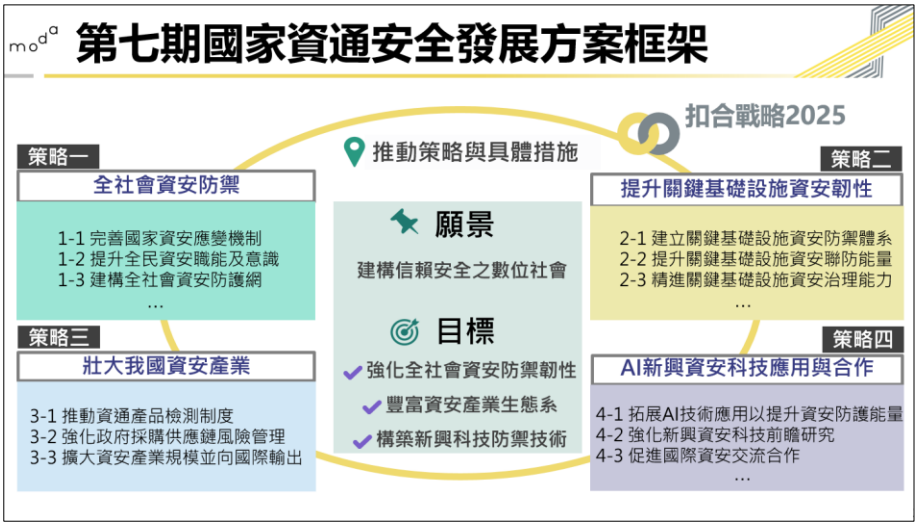
(四)民航局及所屬單位資安韌性體系

1. 上位政策與計畫

資通安全事件已不再僅屬資訊管理議題，而是直接影響機場持續營運、飛航安全與國家關鍵基礎設施防護能力的重要災害型態。因此，資安韌性也被視為機場防災韌性不可分割的一環，需納入機場整體防災架構中加以規劃。

數位發展部配合國家資通安全辦公室「國家資通安全戰略 2025」願景，依《第七期國家資通安全發展方案(114 年-117 年)》〔34〕擬定策略，其中「提升關鍵基礎設施資安韌性」策略之下，訂定了建立關鍵基礎設施資安防禦體系、提升關鍵基礎設施資安聯防能量與精進關鍵基礎設施資安治理能力等具體措施(如圖 17)，預期資安檢測需涵蓋至少 6 個領域，這也是當前民航局執行資安韌性的核心上位計畫。

另外，數位發展部資通安全署的「關鍵資訊基礎設施資安防護建議」〔35〕蒐集世界主要國家與國際工業控制系統資安標準，以及相關防護建議與標準等文件，提出通用性防護建議，提供關鍵基礎設施提供者(如:機場單位)用以擬定「資通安全維護計畫」。



資料來源：〔34〕。

圖 17 第七期國家資通安全發展方案框架

2. 民航局-資安監理與政策制定

民航局做為目的事業主管機關，負責整體民航領域的資安管理政策與法規制定，主要遵循《國家民用航空安全計畫(SSP)》，依據《資通安全管理法》，訂定航空領域的資安維護計畫指引，確保業者遵循國家資安標準，定期對桃園機場公司及航空公司進行資安實地稽核，評估其核心資通系統的防護等級及應變計畫，並將主要機場與飛航管制系統納入「關鍵資訊基礎設施」(CII)，並要求進行年度資安演練，以 確保航空系統及運作安全,重點在於建立航空組織的安全管理系統(SMS)，包含風險管理、漏洞通報、教育訓練、定期評估與強化資安措施(如新一代航空情報系統)，以應對現代網路威脅，保障飛航安全及國家安全。

3. 民航局飛航服務總臺-航管系統韌性與資通安全維護

民航局飛航服務總臺有鑑於近幾年來國內外駭客攻擊事件日新月異、有增無減，社交工程、勒索軟體、機密資料竊取等攻擊事件層出不窮，因此推動資通安全短中長期精進計畫，持續進行資安防護改善作為，以提升系統韌性與資通安全。113-114 年為該計畫中期，計畫目標與工作摘要如下：

1. 擴大且積極培育資安專業人才。
2. 推動資安治理成熟度達第 3 級。
3. 建立終端設備偵測及應變機制(EDR)。
4. 輔導「航空氣象現代化作業系統汰換及更新計畫」導入 ISO 27001 安全管理系統及納入驗證範圍。
5. 建立營運科技(OT)設備資安防護措施。
6. 自行建置弱點掃描軟體平台。

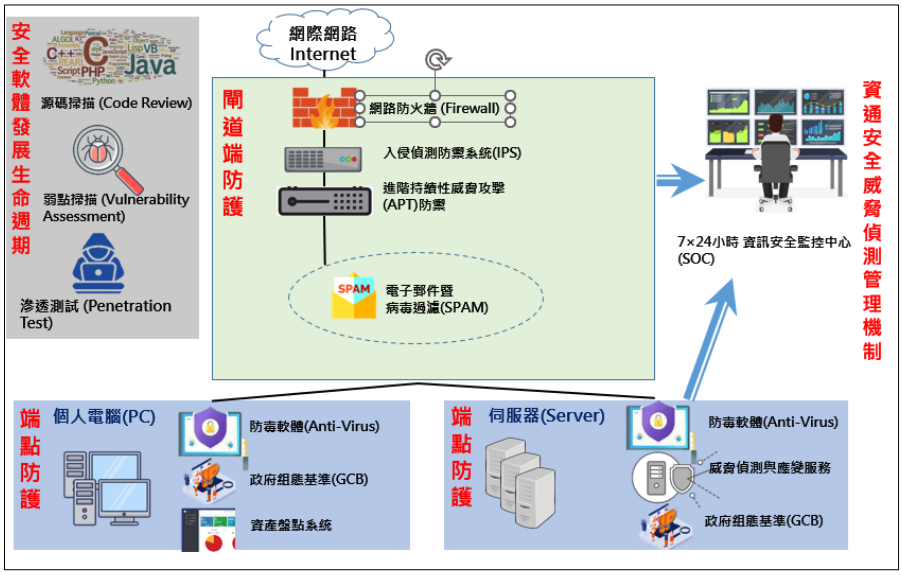
4. 航空站(機場)-區域資安日常系統維運與防護

由民航局直接管轄的各航空站，主要負責區域層級的資安日常系統維運與防護，執行航空站內基礎設施(如場站監控、廣播系統)的資安防護措施。發生資安事件時，需依規定時限向民航局及行政院資安通報及實體呈報；並定期對站內員工進行資安通識教育，提升對社交

工程攻擊的警覺性。

5. 桃機公司-自主資安防護與應變

桃園機場公司為國營事業法人，負責臺灣最大關鍵基礎設施的資安維運，包括建立資安監控中心 (SOC)，透過 24 小時監控即時偵測並阻斷針對機場導航、電力或通關系統的威脅；建立該機場專屬的資安整合平台，與各駐場單位(如航警、海關)共享威脅情資；並取得國際驗證，持續維持 ISO 27001 資訊安全管理系統認證，並針對 2025 年新興威脅(如 AI 攻擊、關鍵資產勒索)更新防護策略。該公司網路及資安防護架構詳如圖 18 所示。



資料來源：桃園機場公司。

圖 18 桃園機場公司網路及資安防護架構

七、我國機場防災韌性課題及精進方向

本研究經回顧國際與我國防災韌性相關文獻及我國機場防災法規與組織體系實務運作，並於 114 年 12 月訪談民航局、桃機公司、飛航服務總臺、臺北國際航空站及所外專家學者，彙整我國機場防災韌性相關課題，並建議精進方向如下：

(一)由「法規遵循」轉向「韌性導向管理」，並建立機場防災韌性評估制度

1. 現行災害防救制度偏重計畫是否完備、程序是否符合規定，並以

「符合法規、完成計畫、通過稽核」為推動核心，較少從「整體系統韌性」角度進行評估，以利進行機場中長期規劃與投資配置。

2. 目前機場較缺乏跨構面、可比較的韌性績效評估，不同機場防災能力難以進行系統性比較，也較少針對不同災害情境下的實際效能、復原速度與跨系統協調能力進行量化評估，亦不利於辨識關鍵脆弱環節與資源投入之優先順序。
3. 現行評估多以單一災害或單一單位為範圍，較少納入多構面整合評估，較難反映機場在面對複合型災害時之整體承受與復原能力。
4. 因此，建議由民航主管機關統籌，建立「機場防災韌性評估制度」，導入多準則評估方法，系統性評估機場整體韌性水準，以做為政策決策與投資配置之重要依據。

(二)強化民航局之整體韌性治理與跨機關整合功能

1. 目前我國機場防災相關制度分屬災害防救、營運持續計畫(BCP)、資通安全及國家關鍵基礎設施(CIP)等不同體系，雖各有法源依據，但在實務運作上仍存在橫向整合不足之情形。
2. 民航局是民航主管機關，除既有監理與督導職能外，可再強化「機場防災韌性」統籌角色，以整合不同制度與資源，避免重複投入。
3. 建議由民航局建立跨機關協調機制，強化與中央災害防救體系、資通安全主管機關及地方政府之連結，形成以航空體系為核心之防災韌性治理架構。

(三)深化營運持續計畫(BCP)，由文件管理轉向情境導向驗證

1. 現行機場 BCP 多著重於文件完備與定期演練，惟在情境設計上，仍以單一事件或既有案例為主，較少針對高衝擊、低發生頻率之極端或複合型災害進行測試。
2. 在極端氣候事件、長時間停電及資通安全事件頻傳之背景下，單一災害情境已難以反映實際營運風險，BCP 若未納入複合型災害考量，將影響其實際可行性。
3. 建議將複合型災害(如天然災害結合資安事件或關鍵系統故障)正式納入 BCP 規劃與演練範圍，透過情境模擬與壓力測試方式，驗證關鍵服務持續能力與復原時效。

(四)將機場防災韌性更明確納入國家關鍵基礎設施(CIP)防護體系

1. 機場與飛航服務系統具備高度關鍵性，其營運中斷將對國家安全、經濟活動與公共秩序產生連鎖影響，已符合國家關鍵基礎設施之核心特性。
2. 現行 CIP 防護機制多著重於設施防護與通報機制，對於「持續服務能力」與「快速復原能力」之評估相對有限，尚未完全反映防災韌性概念。
3. 建議於 CIP 評估與演練中，納入機場防災韌性指標，如關鍵服務復原時間(RTO)、備援系統啟動能力及跨機構協同應變能力，以提升整體防護層級。

(五)強化資通安全韌性，納入機場整體防災韌性架構

1. 隨著機場營運高度數位化，資訊系統與營運技術系統(IT/OT)已成為維持機場正常運作之關鍵基礎，其資通安全事件所造成之衝擊，已具備災害性質。
2. 目前資通安全管理多獨立於防災體系之外，未完全納入整體防災韌性架構中進行整合評估，恐造成制度與實務落差。
3. 建議將資通安全事件正式視為機場災害類型之一，並納入防災韌性評估、BCP 規劃及演練體系中，強化機場在資安事件下之持續營運與快速復原能力。

八、結論與建議

(一)結論

1. 綜合 CDRI 所提出之「邁向韌性機場五大步驟」及 FAA 推動之韌性管理計畫，可知國際機場防災思維有以下轉變：

(1)制度層面：由符合法規轉向韌性導向評估制度

CDRI 所提出之定期脆弱度評估與制度化、循環式的全面性韌性評估，顯示國際機場防災管理已從「符合法規」轉向「具備實質韌性」。我國現行制度多數以法定演練為核心，顯示制度設計上需注重制度化的定期韌性評估與成果回饋機制。

(2)治理層面：由單位防災轉向跨關鍵基礎設施整合

CDRI 建議之跨利害關係人合作與整合防災韌性計畫，顯示機場韌性高度依賴外部系統。我國機場防災可考量朝向跨部門、跨系統整合方向發展。

(3)營運與技術層面：由事件應變轉向全生命週期韌性管理

FAA 提出之韌性管理計畫，將慢性壓力源與日常營運納入防災韌性核心，與傳統聚焦突發事件的防災思維有所不同。此一觀點對我國機場具有高度啟示性，特別是在數位化依賴與設施新舊並存下，除強化應變能力外，亦須將韌性概念制度化嵌入營運管理、資產規劃與人力培育體系中。

(4)決策層面：由經驗判斷轉向風險承受度導向決策

CDRI 提出之風險承受度概念，為機場在不確定風險情境下提供明確決策基準，使投資、防護與調適策略能在成本效益與風險控制間取得平衡。我國在防災投資與韌性資源配置上，現行決策多仰賴個案判斷或行政裁量，缺乏制度化風險界定，後續可考量引入風險承受度概念，以提升決策透明性與一致性。

2. 在氣候變遷加劇、複合型災害頻繁及航空系統高度數位化背景下，機場所面臨風險已由傳統單一災害，轉變為跨構面、跨系統之複合性衝擊。我國雖已建立災害防救、營運持續計畫(BCP)、資通安全及國家關鍵基礎設施(CIP)等相關制度，然整體仍以「法規遵循」與「計畫完備」為主要推動邏輯，對於機場整體防災韌性之量化評估、跨機場比較及中長期投資決策支援仍有待強化。

3. 機場屬於高度關鍵之交通運輸設施，其防災韌性攸關國家運輸安全、經濟活動與社會穩定。為因應極端氣候、複合型災害及不斷資安攻擊事件，機場防災韌性評估宜建立一套可系統性衡量、比較與持續追蹤機場防災韌性成熟度之制度化評估機制，結合多準則評估工具與情境分析方法，透過系統化指標與量化分析，協助民航主管機關掌握不同機場在災害應對能力的韌性狀況，並對應我國民航災害防救計畫與體系、營運持續計畫(BCP)及國家關鍵基礎設施(CIP)防護制度，以做為政策精進與資源合理配置之依據。

(二)建議

1. 國際防災韌性規劃已轉型為風險導向、系統思維與全生命週期管理，不再僅限於單一設施或應變計畫，而是涵蓋多元面向的整體能力，後續建議可依短、中、長期時程逐步推動:

(一)短期：建立機場防災韌性評估制度

建議導入以風險導向與韌性導向為核心之機場防災韌性評估工具，初期可採成熟度模型或質化指標方式，系統性檢視機場在不同災害情境下之承受能力、應變能力與復原能力，定期檢核各機場整體韌性水準，做為現行機場緊急應變計畫(AEP)、BCP 及相關防災計畫之補充依據，並做為中長期規劃與投資決策之重要參考。

(二)中期：將韌性評估納入決策與營運管理循環

建議逐步將防災韌性評估結果，納入機場投資決策、重大工程規劃、營運持續計畫修訂及演練設計之參考依據，建立「評估—改善—再評估」的循環式管理機制，使防災韌性轉化為持續精進的管理依據。

(三)長期：建構跨關鍵基礎設施之整合防災韌性機制

建議從國家關鍵基礎設施防護體系出發，建立跨機關、跨關鍵系統之機場防災韌性治理平台，推動共同風險評估、資訊共享與聯合演練機制，以強化機場與外部支援系統之整體韌性，俾可因應未來高不確定性與高衝擊之複合型災害風險。

2. 將機場防災韌性明確納入國家關鍵基礎設施防護體系

建議於 CIP 防護與演練機制中，除既有防護與通報要求外，進一步納入機場關鍵服務持續能力、復原時間與備援效能等韌性指標，以確保在重大衝擊下，航空服務仍能維持基本運作。

3. 整合資通安全與防災體系，提升資安韌性

建議將資通安全事件納入防災韌性評估與 BCP 架構中，以強化 IT/OT 系統備援設計、快速復原及跨單位協同應變能力，以因應數位化風險對機場營運之衝擊。

參考文獻

1.MarketsandMarkets, Future of Airport Industry to 2030, 2024.

2.ACI, Global Outlook of Airport Capital Expenditure, 2021.

3.ACI, Airport Economics Report, 2025.

4.CDRI, Global Study on Disaster Resilience of Airports- Five Steps towards Resilience of Airports, 2025.

5.聯合國減少災害風險辦公室(United Nations Office for Disaster Risk Reduction, UNDRR)網頁,擷取時間是 2025 年 3 月 https://www.undrr.org/terminology/resilience.

6.ESA, A Guide for Resilience Planning at Airports, 2022.

7.ICAO, Climate Resilient Airports, 2020.

8.ACI, Airports' Resilience and Adaptation to a Changing Climate, 2018.

9.Eurocontrol, Towards Pandemic-Resilient Airports, 2022.

10.Climate-ADAPT, Adaptation Measures to Increase Climate Resilience of Airports, 2020.

11.ICAO, Airport Services Manual Part 7- Airport Emergency Planning, 1991.

12.ICAO, Airport Services Manual Part 7- Resilience, 2022.

13.ICAO, Cybersecurity Action Plan, 2022.

14.CDRI, Global Study on Disaster Resilience of Airports Phase 1, 2023.

15.ICAO, 2025 ICAO Environmental Report - Skyward Action, Understanding Airport Resilience & Adaptation: Insights from Airport Managers, 2025.

16.ICAO, Guidance Material on Airport Preparedness for Effective Humanitarian Assistance and Disaster Response, 2022.

17.ICAO, ICAO Crisis Management Framework Document (EUR Doc 031) Second Edition, 2023.

18.行政院國土安全辦公室,國家關鍵基礎設施防護-演習參考手冊， 110 年 4 月 9 日修正版。

19. Anne Tiernan et al., A Review of Themes in Disaster Resilience Literature and International Practice Since 2012, 2018.

20.李彥呈,建立混合多準則決策模型評估機場韌性之研究,淡江大學商管學院運輸管理學系碩士論文,2023 年。

21.羅方妤,濟州航空班機墜毀…第 2 個黑盒子找到了！將協助釐清失事謎團，聯合新聞網，2024 年 12 月 29 日。

22. 國家災害防救科技中心網頁，擷取時間:2025 年 4 月。https://den.ncdr.nat.gov.tw/1330/1334/1336/9717/9917/
23. Victoria Shannon，快速了解布魯塞爾爆炸案, 紐約時報中文網，2016 年 3 月 23 日。
24. Ross Wang, 微軟直指歐盟規定導致 Windows 無法及時封阻 CrowdStrike 癱瘓全球 850 萬電腦的事件延燒, 最新科技新聞，2025 年 7 月 22 日。
25. Blogadmin，歐洲機場勒索攻擊：航空業資安的警鐘，竣盟科技，2025 年 9 月 23 日。
26. Wylie Wong, Airports Secure Their IT Operations and Improve Business Continuity, StateTech, April 2025.
27. 行政院國土安全辦公室，國家關鍵基礎設施安全防護指導綱領，114 年 8 月 19 日。
28. 行政院國土安全辦公室，國家關鍵基礎設施防護-演習參考手冊，110 年 4 月 9 日。
29. 中央災害防救委員會，災害防救基本計畫(民國 113 年至 117 年)，112 年 12 月。
30. 中央災害防救會報網頁，擷取時間:2025 年 10 月。https://cdprc.ey.gov.tw/Page/A80816CB7B6965EB
31. 交通部民航局，民用航空局災害防救業務計畫，101 年 5 月 23 日 修訂版。
32. 交通部，2020 年版「運輸政策白皮書」空運分冊，108 年 12 月。
33. 民航局，臺灣地區民用機場 2045 年系統規劃(期末報告書審查會議修正一版)，114 年 10 月。
34. 行政院國家資通安全會報，第七期國家資通安全發展方案(114 年-117 年)，114 年。
35. 行政院資通安全處，關鍵資訊基礎設施資安防護建議，107 年 11 月。